COMBINED INTEROPERABILITY TECHNICAL ARCHITECTURE (CITA)

ACP 140

Version 1.0

3 May 1999

(Published March 2000)

This page intentionally blank

FOREWORD

1. ACP 140, COMBINED INTEROPERABILITY TECHNICAL ARCHITECTURE (CITA), is an UNCLASSIFIED publication. Periodic accounting is not required.

2. ACP 140 will be effective for National, Service, or Allied use when directed by the appropriate Implementing Agency; refer to the National Letter of Promulgation (LOP).

3. This publication contains Allied military information and is furnished for official purposes only.

4. It is permitted to copy or make extracts from this publication without consent of the Authorising Agency.

This page intentionally blank

ACP 140

UNITED KINGDOM NATIONAL LETTER OF PROMULGATION

1. The purpose of this National Letter of Promulgation is to implement ACP 140, COMBINED INTEROPERABILITY TECHNICAL ARCHITECTURE (CITA), within the Armed Forces of the United Kingdom of Great Britain and Northern Ireland.

2. ACP 140 is an UNCLASSIFIED non-registered Allied Communication Publication (ACP) which will be EFFECTIVE WHEN DIRECTED.

3. Comments or recommendations concerning this publication should be forwarded through the normal channels to the Defence Communication and Information Systems Standards Executive Group (DCISSEG), Ministry of Defence, Room 338, Northumberland House, Northumberland Avenue, London WC2N 5BP.

4. Compromise or loss of this publication is to be reported through the normal chain of command to the Ministry of Defence, London.

BY COMMAND OF THE DEFENCE COUNCIL

PERMANENT UNDER SECRETARY OF STATE

This page intentionally blank

ACP 140

RECORD OF CHANGES AND CORRECTIONS

Enter change or correction in appropriate column.

Identification of Change or Correction: Reg. No. (if any) and date of same.		Date Entered	By whom entered (Signature; rank, grade or rate: name of command)
Change	Correction		

A

RECORD OF CHANGES AND CORRECTIONS

Enter change or correction in appropriate column.

Identification of Change or Correction: Reg. No. (if any) and date of same.		Date Entered	By whom entered (Signature; rank, grade or rate: name of command)
Change	Correction		

ACP 140

RECORD OF PAGES CHECKED

(NON-US HOLDERS ONLY)

Date Checked	By Whom Checked (Signature & Rank)	Date Checked	By Whom Checked (Signature & Rank)

Note: To meet local requirements, this page may be replaced when all entries are filled. The publication holder is to arrange local reproduction and certify the replacement pages as a "true Copy." The original page numbers are to be allocated to the copy. Superseded pages should then be destroyed in accordance with applicable National instructions.

A

RECORD OF PAGES CHECKED

(NON-US HOLDERS ONLY)

Date Checked	By Whom Checked (Signature & Rank)	Date Checked	By Whom Checked (Signature & Rank)

Note: To meet local requirements, this page may be replaced when all entries are filled. The publication holder is to arrange local reproduction and certify the replacement pages as a "true Copy." The original page numbers are to be allocated to the copy. Superseded pages should then be destroyed in accordance with applicable National instructions.

ACP 140

TABLE OF CONTENTS

This page intentionally blank

CHAPTER 1

GENERAL

SECTION I - INTRODUCTION

101. BACKGROUND

Fundamental to the definition of interoperability is an understanding of the operational environment within which the CCEB nations will operate and in which interoperability must be achieved.

The operational environment of the future is perceived to be one of coalitions, flexible in their constitution and unlikely to be constrained to CCEB members. Partners will not have common procedures and operational techniques. The operational environment will also need to take into account civil and national influences and the integration of functional elements at all levels of the organisational structure.

The essence of combined interoperability is the ability to integrate command and control systems within this coalition structure. This requirement is the ability to share and actively exploit common information while dynamically developing processes and procedures that are appropriate to the existing coalition.

102. CCEB VISION

The CCEB vision statement adopted by the Principals which describes the goal environment is:

> *"The CCEB is committed to maximising the effectiveness of combined operations by the definition of a Combined Interoperability Environment. This environment will enable users to share, creatively apply and add value to collective information and knowledge, constrained solely by policies defined by originators and recipients."*
>
> *(CCEB Publication 1001)*

The Combined Interoperability Environment goal is to establish an interoperable Communications and Information Systems (CIS) capability, able to support all nations' defence requirements and achieved in an affordable and cost-effective way.

103. PURPOSE OF THIS PUBLICATION

The purpose of the ACP 140 is to provide the technical interoperability standards for achieving the CCEB vision. The primary aim is to facilitate interoperability among CCEB Nations so that their

defence CIS (supporting different elements within the CCEB business) can exchange information and other services in a timely and secure manner, as determined by business and operational imperatives.

In meeting these objectives it is vital that all systems adhere to a common security framework so that each affords appropriate protection to information held within the CCEB CIS federation. Such a federation will be composed of diverse CIS, including fixed and deployed Intranets belonging to the national systems. For joint operations these networks have to be linked together to provide the technical means for interworking.

This publication also seeks to expose some of the rationale supporting the selection of services and standards. The complete rationale is given in the 'CITA Rationale and Development Framework' document, ref. CCEB Publication 1007.

104. NATIONAL COMPLIANCE WITH ACP 140

ACP 140 is intended to guide the planning of acquisition and development of specific service functions within new or upgraded national CIS, where there is a need to interoperate with the systems of other CCEB nations. It should be consulted by project managers and systems designers to ensure compliance with essential aspects of the CITA, and by operational staff seeking to exploit the interoperability provided by the CITA.

ACP 140 is a "forward-looking" document listing the standards agreed for relevant services and interfaces to be used now and in the future. It also serves as a baseline for the migration of existing systems towards CITA compliance. The document provides a CCEB agreed coherent set of services and standards that can be used to support interoperability between CCEB nations. It does not seek to constrain the designer to this set of services and standards when meeting system requirements; the designer is free to use whatever is appropriate within the system. However it does identify the services and standards that must be present at the system boundary in order for interoperability to be realised.

The selected standards do not cover all aspects of CIS, nor do they include all information technology standards used currently within national systems. The CITA is concerned only with services essential for interworking between nations. However, any other standards specified outside the scope of ACP 140 must be additive, complementary, and non-conflictive with ACP 140 and its applicable Annexes and Supplements.

Legacy Systems

If legacy standards are needed to interface with existing systems, they can be implemented on a case-by-case basis in addition to the mandated standards. New systems should aim to be backwards

compatible wherever possible. Legacy systems should aim to migrate towards CITA standards when upgrades are due.

105. DOCUMENT ORGANISATION

Allied Communications Publications (ACPs) provide the specific instructions and procedures essential to the conduct of common military operations. They are prepared in accordance with the format contained in the ACP 198 series.

Sections I - IV of the present document explain the context for ACP 140 and the processes by which CIS standards have been selected to meet CCEB requirements for interoperability. Implementation and Compliance are covered in Section V. Individual CIS service areas are discussed in separate chapters within Section V and detailed technical specifications given for each service area within CITA scope.

106. NATIONAL POINTS OF CONTACT

Each nation has a lead in the development and maintenance of the CITA as follows:

Australia:
Mr. Jed Bartlett
Information Policy and Plans Branch,
Defence Information Systems Group,
Department of Defence,
NCC-B12, Canberra, ACT 2600.
Tel. +61 2 6266 9769
Email: jed.bartlett@cbr.defence.gov.au

Canada:
Maj. Marie-Claire Gosselin-Patterson
Directorate of Distributed Computing Engineering and Integration,
DDCEI 3-3,
National Defence Headquarters,
Ottawa, Ontario, K1A 0K2.
Tel. +1 613 992 5551
Email: ae200@issc.debbs.ndhq.dnd.ca

New Zealand:
Mr. Mark Baddeley
JCIS,
HQNZDF,
Private Bag,
Wellington.

Tel. +64 4 496-0191
Email: markb@jcis.mil.nz

United Kingdom: Mr. Bill Mears
DCISIA - SE
Northumberland House
Northumberland Avenue
London, WC2N 5BP.
Tel. +44 171 21 87458
Email: dcisseg6@dgics.mod.uk

United States: Mr. Charles Schaffer
JS/J6I, C4 Systems Directorate Technology and Architecture Division,
Room 1E833, The Pentagon,
Washington DC, 20340-0001.
Tel. +1 703 614 7005
Email: cschaffer@acm.org

SECTION II - CITA OVERVIEW

107. ARCHITECTURES

An architecture is defined by the Institute for Electrical and Electronic Engineers (IEEE) in IEEE 610.12 as the organisational structure of a system or component, their relationships, and the principles and guidelines governing their design and evolution over time. The CITA has defined an interrelated set of architectures: Operational, Systems, and Technical. Figure 1-2 shows the relationship among the three architectures. The definitions are provided here to ensure a common understanding of the three architectures[1].

[1] These definitions are based on the US definition. In the UK the Operational Architecture is further broken down into the Business Architecture and Information Architecture

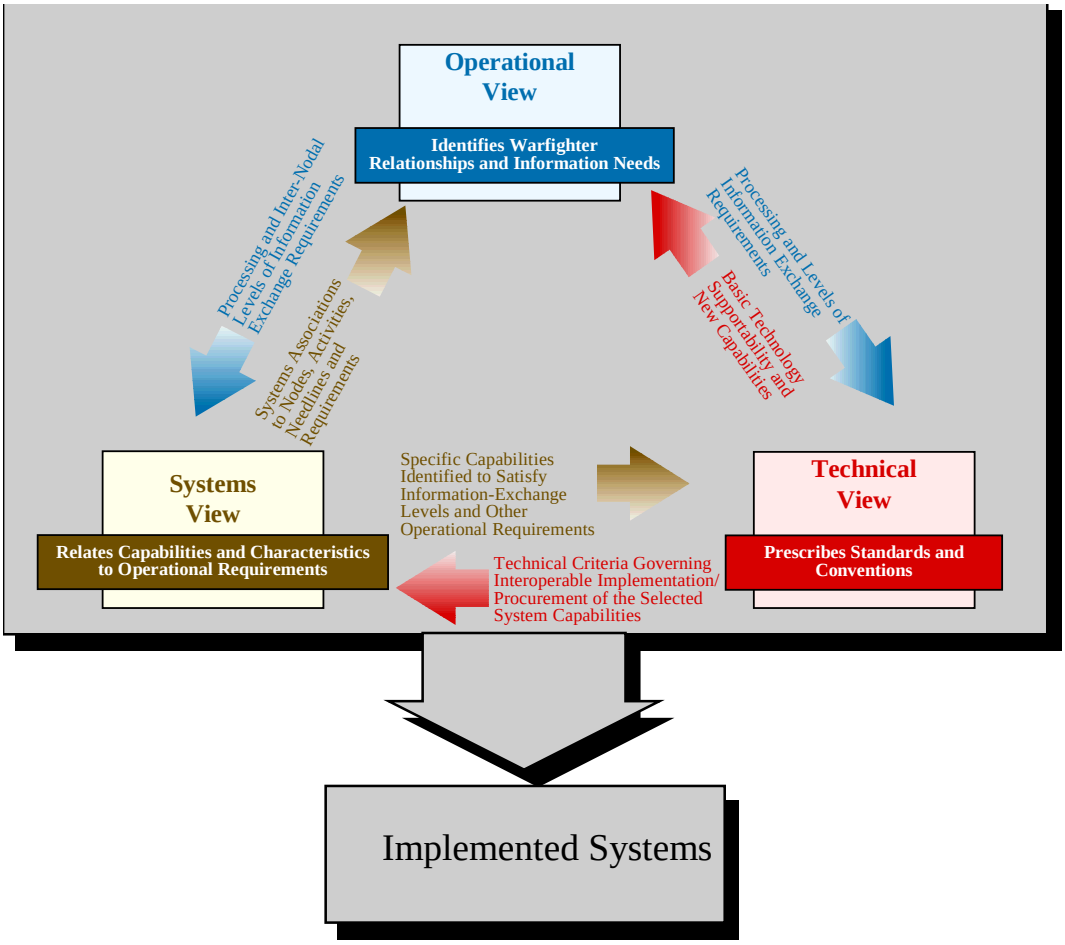

Figure 1-1. Architecture Relationships

a. Operational Architecture View (OA)

A description (often graphical) of the operational elements, assigned tasks, and information flows required accomplishing or supporting the warfighting function. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges.

b. Systems Architecture View (SA)

A description, including graphics, of systems[2] and interconnections[3] providing for or supporting warfighting functions. The SA defines the physical connection, location, and identification of the key nodes, circuits, networks, warfighting platforms, etc., and specifies system and component performance parameters. It is constructed to satisfy Operational Architecture requirements per standards defined in the Technical Architecture. The SA shows how multiple systems within a subject area link and interoperate, and may describe the internal construction or operations of particular systems within the architecture. (C4 Chiefs Consensus SA Definition, 12 January 1996, as modified at the suggestion of the USD(A&T) community).

c. Technical Architecture View (TA)

A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The technical architecture identifies the services, interfaces, standards, and their relationships. It provides the technical guidelines for implementation of systems upon which engineering specifications are based, common building blocks are built, and product lines are developed.

The CITA corresponds to the technical architecture of this model.

108. CITA OVERVIEW

a. Definition

The CITA is the Technical Architecture which contains the technical recommendations for a profile of standards and guidelines for support of essential requirements for interoperability among CCEB nations.

As noted above, a technical architecture is simply a list of information services and their corresponding standards. The intent of standardising on services is to promote interoperability across any systems designed using this architecture. The CITA is the technical architecture endorsed by CCEB nations.

---

[2] Systems: People, machines, and facilities organized to accomplish a set of specific functions, which cannot be further subdivided while still performing required functions. Includes the radios, terminals, command, control, and support facilities, sensors and sensor platforms, automated information systems, etc., necessary for effective operations.

[3] Interconnections: The manual, electrical, or electronic communications paths/linkages between the systems. Includes the circuits, networks, relay platforms, switches, etc., necessary for effective communications.

Although there are many information services that could contribute to interoperability, an attempt has been made to limit recommendations to those services for which an operational requirement currently exists and for which suitably open standards are available. For newer technology services which are not yet part of an operational concept or for which standards are still emerging, some discussion is provided, but no recommendation.

CCEB Publication 1007, *CITA Rationale and Development Framework*, describes the process by which candidate information services were identified and evaluated. In determining the necessity of each service, the following are considered: relevance to interoperability, existence of an inter-nation requirement, and scale of the inter-nation requirement. The feasibility of each service is determined by considering whether there exists an acceptably open standard, the interconnection security policy, legacy issues, cost, risk, and system evolution issues. It is recognised that it is not always advantageous to standardise a particular service.

The standards selection process has sought to adopt wherever possible those services and standards that are dominant in the commercial world and which benefit from wide market support.

The results of the process are summarised in Table CHAPTER 2-2 "CITA Specification (Version 1.0)".

b. CITA Concept of Operations

The CITA is relevant when the need arises to transfer information or share services between a system belonging to one CCEB nation and a system belonging to another CCEB nation. The standards defined in the CITA are required at one of the following:

1. the boundary of the national system (typically a gateway);

2. the interface between a deployed system and the target CCEB system; or

3. within a CCEB coalition system (the national system becomes part of the coalition system).

c. Benefits

The benefits of adopting the CITA result from the advantages of a technical architecture and the use of mainstream commercial products. In summary they are as follows:

- interoperability is promoted when common standards are adopted;

- there is increased scope for the use of commercial, off-the-shelf (COTS) products, hence reduced cost and risk;
- there is a reduced risk of lock-in to a single system provider;
- system evolution is made easier by following commercial developments.

d. Relationship to National Technical Architectures

Clearly, the Nation Specific Interoperability Technical Architectures (NSITAs), and any alternative forms of local agreement relevant to other nations, must embrace the CITA: This concept is depicted in Figure 1-2 below.

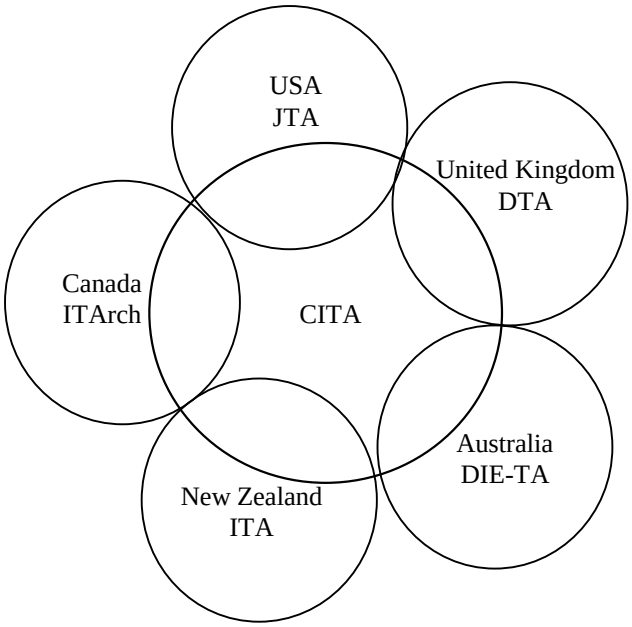

Figure 1-2. Scope of the CITA in relation to other NSITAs

e. Security

The CITA makes no statements about the security architecture or policy to be adopted for end-systems. However, the widespread interconnection of systems envisaged means that secure messaging alone cannot provide adequate protection. Depending upon the protective marking of the data and/or system and the geographical location and nature of the communications bearers, messaging interconnections between systems will continue to

require COMSEC protection through the use of (an appropriate grade of) encryption at the network/link level or at the application layer level. Even where the data exchanged has a low or even no security classification, COMPUSEC concerns, possibly derived from distant systems in the federation, will often lead to a supplementary requirement for network-level encryption.

f. Technical Scope of the CITA

The technical scope of the CITA will establish where the boundary between it and nation-specific ITAs lies. This will depend largely on the interoperability mechanisms CITA aims to employ. A service will be deemed *outside* the CITA if the need to use it (and hence standardise it) arises solely from requirements within individual nation boundaries. Conversely, a service is a *candidate* for standardisation within the CITA whenever there is a significant requirement for exchange of that service between CIS from different CCEB nations.

A balance must be established between the benefits and restrictions of standardisation. Where a limited number of CIS are involved, an ad hoc bilateral, or multilateral, agreement may be preferable. The *principles* by which it is proposed that issues such as these should be decided are discussed in Paragraph 111.

The technical architecture does not constitute a complete specification of the system. The CITA addresses only those elements of CIS that are relevant to interoperability between CCEB nations and these may be a relatively small part of the full system functionality. National ITAs probably go beyond the scope of CITA but they are still limited to interoperability issues.

At the very least, each system will offer applications specific to the needs of its local users. Furthermore, there will be locally required infrastructure services for which standardisation (either within the CITA or a nation-specific ITA) would serve no useful purpose. In these cases, local service agreements will be negotiated between the parties involved and standards chosen according to purely local requirements, taking note of sector level preferences (Land Sea or Air) or, for example ABCA agreements[4].

[4] Of course, what may start out as local agreements may find wider utility. In this case, these local agreements may be adopted and subsumed by the CITA depending on the scale and scope of their applicability. The overall objective is to move towards commonality.

SECTION III - STANDARDS SELECTION PROCESS

109. SELECTION PROCESS OVERVIEW

The CITA standards selection process consisted of the following four stages:

a. CITA Candidate IT Services are identified

b. CITA Scoping Principles are applied

c. CITA Scope is assessed

d. CITA Standards are recommended.

This process is depicted diagramatically below in Figure 1-3.

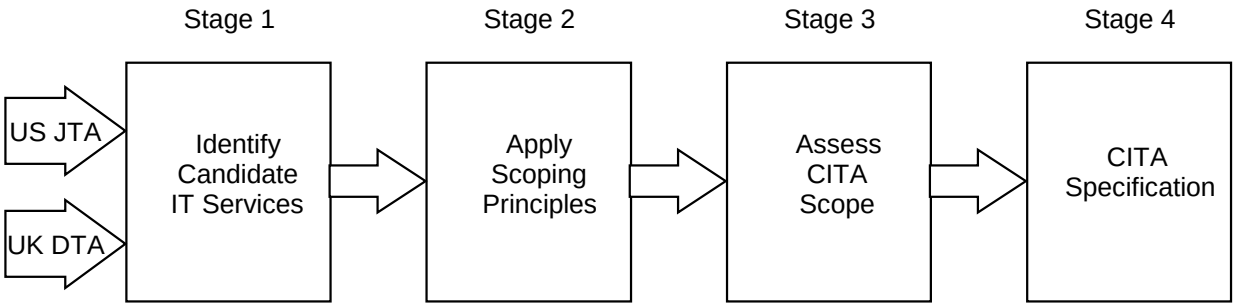

Figure 1-3: Overview of CITA Standards Process

110. CANDIDATE IT SERVICES

The initial set of candidate IT services were selected from nation-specific technical architectures defined by the US and the UK, namely the DoD JTA and the MOD DTA respectively.

The candidate IT services were categorised as follows:

a. Operating Systems Services

This category covers standards for the services provided by computer operating systems and the means of accessing them by user applications.

b. User Interface Services

This category covers a miscellany of standards relevant to the Human-Computer Interface, including look and feel standards/conventions, APIs for windowing systems, desktop managers plus desktop hardware and operating system environments. It includes remote presentation protocols (e.g. X11) and inter-process communication protocols (e.g. DDE) which are also listed under Distributed Computing.

c. Network Services[5]

This category covers the standards for communications-related applications operating at layer 7 of the ISO OSI reference model. It also includes some of the services and protocols required by these applications.

d. Communications

This category covers the standards for transporting data between end systems. It includes the bearers of data, both physical (e.g. fibre-optic) and non-physical (e.g. RF).

e. Distributed Computing

This category covers the services required to access and distribute information, resources and processing across a federation of systems.

f. Data Management Services

This category covers the services required to manage shared data, data dictionaries and databases. It includes the services required for database replication and remote data access.

g. Data Interchange

This category covers the standards for the interchange of information between systems and applications. It can include standards that are supported natively by several applications as well as intermediate standards that applications can convert both to and from

h. System and Network Management

This category covers the services required to effectively manage the configuration, security and faults of end systems and their interconnecting networks.

---

[5] Network services do not equate to the ‘Network Layer’ in the OSI model.

i. Software Engineering

This category mainly covers standards for the system/software lifecycle processes and associated tools but also includes standards for programming languages and their bindings.

j. Graphics

This category provides standards for graphics services providing users and user applications with the means to create, store, access, manipulate, display and print graphic images.

k. Internationalisation

This category covers standards and conventions that facilitate the use or re-use of systems or software within different National or cultural contexts.

l. Security Services

This category covers the services required to provide secure communications between CIS. They also provide services for detecting and preventing hostile manipulation and attack of CIS.

m. Support Application Software

This category covers general-purpose or utility applications software. A variety of application types are included under this heading . Those covered explicitly under this heading are OA applications and those categorised as transaction processing applications.

n. Collaborative computing

This category covers services and applications that support group-working by spatially separated individuals. They promote the ability of coalition forces to collaborate using their respective CIS.

o. Special Application Software

This category covers system or mission-specific applications software which would only be expected to be found on systems performing a similar role.

111. SCOPING PRINCIPLES

The resultant set of IT services that passed through the first filter were then scrutinised against a set of scoping principles. These principles were designed to evaluate whether an IT service should be considered by the CITA for possible standardisation. The scoping principles used were as follows

a. **Inter-Nation requirement**: is there genuine evidence of an existing or emerging requirement to exchange this service across systems from different nations?

b. **Openness**: is there an open solution available to provide this service or are there overriding business or operational reasons for adopting a non-open solution?

c. **System boundary issues**: which parts of a standard, or what types of standard, are applicable to the specification of external system interfaces?

d. **Legacy issues**: are there practical concerns related to legacy systems that would limit standardisation or suggest a preferred standard?

e. **Cost/risk**: are there significant cost and risk implications of standardisation in this area?

f. **Interconnection security policy**: are there likely to be interconnection security policy constraints that would prevent systems exchanging these services, or the adoption of particular standards?

g. **System evolution**: do system evolution imperatives dictate that standardisation is not feasible, or that multiple versions of any given standard need to be supported concurrently?

112. ASSESSMENT OF SCOPE

Having applied the second filter, the resultant IT services were analysed and a potential set of standards identified. From the potential standards, well defined, well supported and reasonably stable standards were allocated to the CITA IT services. Also identified were emerging CITA IT standards that were considered too immature at present for inclusion now, but were expected to become dominant in the near term. In a number of cases there are a number of competing, emerging standards. Further market analysis is required before a decision can be made for their inclusion into the CITA.

SECTION IV - IMPLEMENTATION

113. APPLICABILITY AND COMPLIANCE

The CITA is applicable to national CIS that are required to participate in a CCEB-wide CIS federation, exchanging information across national boundaries and possibly between CCEB nation forces during combined operations. However, not every participating CIS will necessarily implement the whole of the CITA because national operational requirements for that CIS may not require all the CITA services or its services are supported with other products.

The extent to which a particular system implements the CITA services determines its scope for interoperability with other CITA-compliant systems. A fundamental principle of CITA compliance is that where a CIS offers a service for interworking across CCEB nations, that service will be implemented according to the CITA specification. However, there will be different levels of CITA compliance according to the actual services involved.

a. Acquisition

CCEB nations must include checks within their CIS procurement procedures to ensure that when participating systems are developed or modified, they are compliant with the CITA according to the claimed interoperability level. Typically this will involve four stages:

1. Before a system is developed or modified, the project manager will create a CITA-compliant standards profile for the system which will be continually updated as the project proceeds;

2. The system developer will select specific options within the CITA standards used by the system in order to provide the necessary functionality and interoperability level;

3. The standards profile will be submitted for internal approval. If any waivers are granted on CITA-specified standards for whatever reason, the CITA WG should be informed so that the impact of non-compliance on CCEB federation interoperability can be assessed;

4. After approval, the standards profile should form an integral part of the procurement specification and confirmation should be sought, by inspection and testing, that the standards are implemented correctly in the delivered system. Periodic monitoring of the system during its service life should be undertaken to see that CITA compliance to a given interoperability level is maintained.

b. Interoperability levels

Interoperability levels have been agreed by the CITA group. A progressive scale of CIS

functionality has been defined with identified points on the scale corresponding to common system capabilities. The lowest levels of the scale will apply to systems offering basic interconnection and simple data exchange, whilst the upper end of the scale will be used to describe sophisticated systems with full network interconnection, able to work with complex data objects across the CIS federation[6].

The interoperability levels are shown in Table CHAPTER 1-1.

Table CHAPTER 1-1

Interoperability Level	Name	Description
1a	Basic document exchange	OA document interchange, hypertext, character sets/alphabets, graphics/still and moving images, file compression, page description, security labelling, accounting and audit.
1b	Full document exchange	As for 1a plus military transfer formats, military symbols (codes only) and standard data products.
2a	Network connection	Inter-networking, transport and domain name services.
2b	Basic Intranet connection	File transfer and interpersonal email with attachments[7].
2c	Web connection	Hypertext transfer, on-line publishing and news group services. Security labelling syntax, semantics and positioning within published documents. Also web authentication and access control mechanisms.
2d	Organisational messaging	Organisational messaging based on X.400 as defined in ACP 123. Also messaging security services.
2e	Directory services	Directory services based on X.500 as defined in ACP 133.

[6] It is possible that hardware compliance will have to be addressed separately from service compliance; these matters are still under discussion.

[7] At present there is no agreed CCEB requirement for interpersonal email.

Interoperability Level	Name	Description
3a	Secure database access/exchange	Database management, remote database access, data dictionary, CCEB data model and associated security services.
3b	Distributed applications	Distributed computing, object interfaces and object middleware if relevant. Also database replication, information sharing, collaborative computing and special applications.

Level 1 compliant systems can read and write files in the formats cited; transfer is either manual or through dedicated links.

Level 2 compliant systems should be able to connect to a CCEB Intranet and perform web access, email, and formal messaging. Level 1 and 2 together broadly equate to NATO level 4 interconnection.

Level 3 compliance is outside the current CITA scope but should fall within the emerging CITA.

A statement showing the level of compliance with CITA will be required for every participating national CIS, so that its scope for interoperability within the CCEB federation becomes apparent. Nations will assume responsibility for carrying out compliance checks on their own systems and issuing compliance statements to the CITA WG. Ideally, compliance with at least one of the defined CITA levels should be mandatory but allowance will have to be made for possible exceptional factors until experience with CITA systems has been gained.

114. CITA EVOLUTION

The CITA will be kept under review and changes introduced to the specification in response to new CCEB requirements and technology developments. Service areas presently outside the scope of CITA should be monitored for possible inclusion, while the standards for existing services must reflect changes in the market. Market movements will affect the feasibility of implementing services in accordance with open standards and this factor must be taken into account in revising the CITA specification. The need to retain backwards compatibility is recognised; market forces and the need to retain a customer base will frequently ensure that commercial products are compatible with earlier versions as well as competing products.

A major change driver will be feedback obtained from projects compliant with the CITA. Nations must establish mechanisms, if not already in place, for eliciting feedback and passing relevant information to the CITA WG to assist CITA management. In any event, evolution of the CITA specification will have to take into account changes to national technical architectures where they relate to CITA functionality.

The CITA WG will monitor these change drivers and update the CITA as appropriate.

Proposed changes and comments are to be put to national contacts. These will be considered on a regular basis by the CITA Working Group and appropriate action taken.

This page intentionally blank

CHAPTER 2

CITA SPECIFICATION SUMMARY

201. CITA SPECIFICATION

Table CHAPTER 2-2 summarises the recommended standards profiles for the CITA. The services have been grouped into 15 broad categories. For each service, there is a recommendation for a standard. A more detailed rationale for selecting that standard is included in CCEB Publication 1007.

202. KEY DRIVERS

A key driver in the process of selecting the CITA services has been the existence (or likely existence) of user requirements and whether or not the technology exists to provide those services. The selection of standards for the CITA specification has been driven by the following:

a. **adoption of Internet and web technologies.** The CITA cites the popular internetworking standards TCP, IP and UDP; the data exchange protocols in widespread use on the Internet and in commercial networks (HTTP, NNTP, FTP etc.); and common data interchange formats (HTML, JPEG, zip, etc.);

b. **need for security.** The most significant departure from commercial standards is in the adoption of a common security protocol (ACP 120) particularly in support of messaging. A common approach to secure messaging is fundamental to the existence of an effective CITA;

c. **adoption of essential requirements to meet military needs.** Common elements of CCEB standards for organisational messaging (ACP123) and directory (ACP133) are adopted.

203. CITA SERVICES OUT OF SCOPE

A number of CITA services are currently ruled out of scope; they are not shown in the specification summary but are listed below. Services are ruled out of scope if there is no inter-nation requirement or there are no acceptable standards. The scope of CITA services will be kept under review by the Working Group.

Table CHAPTER 2-1

No.	Service Area	Service	Ref Para	Page
1.	Operating System Services		301.	3-1
2.	User Interface Services		401.	4-1

No.	Service Area	Service	Ref Para	Page
3.	Distributed Computing	Distributed process	703.	7-2
4.		Remote presentation	704.	7-3
5.		Distributed file services	705.	7-4
6.		Distributed time services	706.	7-4
7.		Distributed print services	707.	7-6
8.		Distributed transaction processing	708.	7-6
9.		Distributed object services (object middleware)	710.	7-8
10.		Distributed system management	711.	7-9
11.	Data Management Services	Data dictionary services	804.1	8-4
12.		Database management services	804.2	8-4
13.	System and Network Management	System management	1002.	10-1
14.		LAN management	1003.	10-1
15.		National WAN management	1004.	10-2
16.		Communications bearer system management	1006.	10-4
17.	Software Engineering Services		1101.	11-1
18.	Graphics	Graphics programming languages and APIs	1202.	12-1
19.		Application software having a drawing capability	1203.	12-2
20.	Internationalisation		1301.	13-1
21.	General Security	Security domian mediation	1509.	15-9
22.	Support Applications Software		1601.	16-1
23.	Collaborative Computing	Workflow services	1702.	17-1
24.		Whiteboarding	1705.	17-4
25.	Special Applications Software	Geographical Information Systems	1802.	18-1
26.		Track management	1803.	18-2
27.		Alert services	1804.	18-3
28.		Data fusion	1805.	18-4

204. MULTIPLE STANDARDS

The CITA specification generally identifies a single standard or group of interdependent standards for each service. In some cases, however, the Working Group agreed that it would be appropriate to specify multiple standards which progressively add functionality (e.g. HTML, XML & SGML). In such cases a primary standard is identified (HTML in this example) and must be supported regardless of whether any other standards are implemented.

205. CITA SPECIFICATION - VERSION 1.0

Table CHAPTER 2-2

No.	Service Area	Service	Recommended Standard	Emerging Standards	Ref Para	Page
1.	Network Services	Messaging: Organisational	Message transport submission & delivery (P1/P3/P7) ACP 123 Annex C. Gateway between MMHS and ACP127 to be defined. Content Type (P772, ACP 123 Annex A, Annex B, Annex D) Message Store Attributes (P772, MS Attributes, ACP 123 Annex E, Annex F)		502.	5-1
2.		Messaging: Interpersonal	There is presently no agreed requirement for interpersonal messaging. SMTP (RFC 821) + MIME (RFC 2045) are recommended where used.		502.	5-1
3.		Messaging: Naming and Addressing	ACP 123 (based on X.400). ACP 133 (based on X.500).	SMTP addressing schema will need to be formulated as per ACP133.	502.	5-1
4.		Directory	ACP 133 (based on X.500 1992 with some 1997 extensions).		503.	5-3
5.		Naming and Addressing services	DNS (RFC 1035). Internet domain naming policy.		504.	5-4
6.		Remote Terminal services	TELNET (RFC 854/855)		505.	5-5
7.		File Transfer services	FTP (RFC 959) and HTTP v1.1 for file transfer - (Netscape Navigator and MS Internet Explorer and their interoperable proprietary extensions). FTP products that implement the 'Restart' elements of RFC 959 for file transfer in constrained environments.		506.	5-6
8.		ISO services on top of the transport layer	RFC 1006.		507.	5-7

No.	Service Area	Service	Recommended Standard	Emerging Standards	Ref Para	Page
9.	Communications	Telephony	**Secure telephony:** STU-IIB compliant equipment. **Insecure telephony:** Standards selected from ITU-T Recommendations: Series E; Series G; Series P; Series Q; Series V. V.34 for modems. V.42 for communications compression	STE (Secure Telephone Equipment). Voice-over-IP standards. V.90 modem standard (56 Kbits/sec).	603.	6-2
10.		Wide area networks	Internetworking - IPv4 (RFC 791). X.25 + X121 Addressing policy. ISDN - ITU-T I. series of standards. B-ISDN (ATM) - ITU-T I. series of standards + ATM Forum af-standards for physical and adaption layers and LANE v 2.0. SONET/SDH - ANSI T1.105. X.121 addressing policy.	IPv6 (RFC 1883).	604.	6-3
11.		Point-to-Point	RFC 1661/1662 (PPP) RFC 1332 (PPP Internet Protocol Control Protocol (IPCP)) RFC 1989 (PPP Link Quality Monitoring) RFC 1994 (PPP Challenge Handshake Authentication Protocol (CHAP)) RFC 1570 (Link Control Protocol (LCP) Extensions).		605.	6-5

No.	Service Area	Service	Recommended Standard	Emerging Standards	Ref Para	Page
12.	Communications (cont.)	Tactical Data Links	**Link 11** STANAG 5511 annex B, Radio performance & protocols; vol.2, Link 11B Waveform protocol changes. MIL-STD-118-2031a, Conventional Link 11 Waveform 16 tones. SPAWAR-5-850, Single tone Link 11 Waveform. **Link 16** STANAG 4175 edition 1. **Link 22** UHF: STANAG 4372 (Saturn); Saturn can also carry Link 11 and Link 16 messages. HF: STANAG 4444 (Slow hop ECCM). **Link forwarding:** STANAG 5616.	VMF.	606.	6-6
13.		Internetworking Standards	IP v4 (RFC 791). Awaiting CCEB policy on IP addressing.	IPv6 (RFC 1883).	607.	6-7
14.		Transport	TCP (RFC 793) UDP (RFC 768).		608	6-8
15.		Routers	RFC 1812 - Requirements for IP Version 4 Routers Border Gateway Protocol 4.		609.	6-9

No.	Service Area	Service	Recommended Standard	Emerging Standards	Ref Para	Page
16.	Communications (cont.)	SATCOM bearers	**General** MIL-STD-188-146 Interoperability And Performance Standards For Satellite Communications, 15 June 1998. **UHF** MIL-STD-188-181A, Interoperability Standard for Single Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 31 March 1997. MIL-STD-188-182A, Interoperability Standard for 5-kHz UHF DAMA Terminal Waveform, 31 March 1997. MIL-STD-188-183, Interoperability Standard for 25-kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992; with Notice of Change 1, 2 December 1996 (STANAG 4231). MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993. MIL-STD-188-185, DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996. **SHF** MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995. MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995. **EHF** MIL-STD-1582D, EHF LDR (Low Data Rate) Uplinks and Downlinks, 30 September 1996; with Notice of Change 1, 14 February 1997 (STANAG 4233). MIL-STD-188-136, EHF MDR (Medium Data Rate) Uplinks and Downlinks, 26 August 1995; with Notice of Change 1, 15 August 1996, and Notice of Change 2, 14 February 1997 (STANAG 4522).		610.	6-9

No.	Service Area	Service	Recommended Standard	Emerging Standards	Ref Para	Page
17.	Communications (cont.)	Radio bearers	**LF/VLF** MIL STD 188-140A, Equipment Technical Design Standards for Common Long Haul/Tactical Radio Communications in the LF Band and Lower Frequency Bands. **HF** MIL STD 188-141A , Interoperability and Performance Standards for Medium and High Frequency Radio Equipment Standard. STANAG 4203 Technical standard for single channel HF radio equipment. **VHF** MIL STD 188-242, Tactical Single Channel (VHF) Radio Equipment. STANAG 4204 Technical standard for single channel VHF radio equipment. **UHF** MIL STD 188-243, Tactical Single Channel (UHF) Radio Communications. STANAG 4205 Technical standard for single channel UHF radio equipment. **SHF** MIL STD 188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment. **CNR (Voice only)** CNRs are only interoperable for fixed frequency (VHF) voice communications only. There are no commonly agreed standards for frequency agility. The standards are: QSTAG 734 (STANAG 4204) Technical Standards for Single Channel VHF Radio Equipment. **QSTAG 1108 (STANAG 4197A) Common Critical Crypto Standards for Single Channel Communications (Voice, Teletype and Data) for VHF CNR.**	CNR - **Joint Tactical Radio (JTR).**	611.	6-11

No.	Service Area	Service	Recommended Standard	Emerging Standards	Ref Para	Page
	Communications (cont.)	Radio bearers (cont.)	**Data modems** MIL-STD-188-110A Interoperability and Performance Standards for Data Modems. STANAG 4285 Characteristics of single tone modems for HF radio.		611.	6-11
18.		Cable bearers	RS-232, RS-422, RS-423, RS-530; EIA - 4920000-A; EIA - 5090000. Other standards covered under wide area networks.		612.	6-13
19.	Distributed Computing	Distributed database management services	(See under Nation-level Data Management, para 804).		702.	7-2
20.		Object Interchange services	CORBA/IIOP v 2.2; DCOM.		709.	7-7
21.	Data Management	Remote data access	ODBC v 2.	ODBC v 3; JDBC; HTTP-based protocols.	802.	8-1
22.		CCEB level data management	Standards yet to be defined. Data definitions should focus on those data items for which there is an inter-nation exchange requirement.	NATO Core Data Model	803.	8-2
23.	Data Interchange	Business-transaction-oriented data interchange standards	STEP/ISO 10303 for product data; UN/EDIFACT/ISO 9735 for EDI.		903.	9-6
24.		Military data interchange standards	STANAG 5511 (Link 11 standard); STANAG 5516 (Link 16 standard); STANAG 5522 (Link 22 standard); OTHT-Gold; ADatP3 (STANAG 5500).	VMF.	904.	9-7
25.		Office Automation interchange formats	**Primary Standard** MS Office 95 interchange formats preferred. **Secondary Standard(s)** Rich Text Format (RTF) for documents if MS Office 95 format not available. Portable Document Format (PDF).	MS Office 97 interchange formats	902.1	9-2

No.	Service Area	Service	Recommended Standard	Emerging Standards	Ref Para	Page
26.	Data Interchange (cont.)	Hypertext interchange formats	**Primary Standard** HTML v4.0 (Dynamic HTML). **Secondary Standard(s)** SGML for high value, complex publications; XML where meta-language data definitions are required.	XML replacing HTML as primary standard.	902.2	9-4
27.		Hypertext transfer protocols	HTTP v1.1. HTTP with Distribution and Replication Protocol for use in constrained environments.	HTTP V 2.0.	902.3	9-5
28.		Character sets and alphabets	International Alphabet 5 (ASCII).		905.	9-8
29.		Encoding standards	**Data Encoding Standards:** UUENCODE; MIME; SMIME; zip. **Voice encoding standards:** A-law and μ-law (ITU-T G.711). CELP.		906.	9-9
30.		Fax	**Secure fax:** STU-IIB compliant equipment. **Insecure fax:** Group 3 & Group 4.	**Secure fax:** STE.	907.	9-11
31.		Video conferencing	ITU-T H.320, ITU-T H.221, ITU-T H.242, ITU-T H.261, ITU-T H.230, ITU-T H.231, ITU-T H.243, ITU-T H.233, ITU-T H.234, ITU-T H.244.	ITU-T H.323 with ITU-T T.120	908.	9-12
32.		Graphical/still image data interchange standards.	JPEG File Interchange Format v1.02; GIF Version 89a, July 1990.	PNG.	909.	9-13
33.		Geospatially referenced data interchange standards	DIGEST v 2; S-57 edition 3.		910.	9-14

No.	Service Area	Service	Recommended Standard	Emerging Standards	Ref Para	Page
34.	Data Interchange (cont.)	Moving image and audio/visual data interchange standards.	CDFS (ISO 9660); PCM for audio (ISO 11172-3); MPEG2 (video).	ITU-T H.323 with ITU-T T.120	911.	9-16
35.		Audio data interchange standards	PCM (ISO 11172-3).		912.	9-17
36.		File compression standards	zip.		913.	9-18
37.		Page description	**Primary Standard** PostScript (Level I and II); EPS. **Secondary Standard(s)** PDF.		915.	9-19
38.	System & Network Management	CWAN	Procedures defined by Quad C.		1005	10-2
39.	Graphics	Military symbology standards	MIL-STD-2525A (Symbol codes only).		1204.	12-2

No.	Service Area	Service	Recommended Standard	Emerging Standards	Ref Para	Page
40.	Message Security Services	Message origin authentication	ACP 120 (based on X.509 authentication framework).		1402.	14-1
41.		Message access control	Syntax of security label currently being prepared by the CMI WG of the INFOSEC ISME.		1403.	14-3
42.		Message content privacy/confidentiality	Based on X.509 authentication framework.		1404.	14-4
43.		Message content integrity	ACP 120.(based on X.509 authentication framework).		1405.	14-5
44.		Certificate management and distribution	X.500 and ACP 120.(based on CMI X.509 authentication framework).		1406.	14-6
45.		Message non-repudiation with proof of origin	ACP 120 (based on digital signatures within the CMI Authentication Framework and associated PKI).		1407.	14-7
46.		Message non-repudiation with proof of delivery	ACP 120 (based on digital signatures within the CMI Authentication Framework and associated PKI).		1408.	14-8
47.		Message accountability	ACP 120 (based on digitally signed receipts and PKI).		1410.	14-9
48.	General Security	Authentication	X.509 - Awaiting CCEB policy.		1502.	15-1
49.		Access control	Awaiting CCEB policy.		1503.	15-3
50.		Key management and distribution	Awaiting CCEB policy.		1504.	15-4
51.		Data confidentiality	ACP 120 application layer data confidentiality or link level encryption.		1505.	15-5
52.		Data integrity	ACP 120 application layer data confidentiality or link level encryption.		1506.	15-6
53.	Collaborative Computing	On line wide-area publishing services.	**Primary Standard** HTTP(v1.1)/HTMLv4.0. **Secondary Standard(s)** SGML for high value, complex publications; XML where meta-language data definitions are required.		1703.	17-2
54.		News Group services	NNTP (RFC 977).		1704.	17-3

This page intentionally blank

CHAPTER 3

OPERATING SYSTEMS SERVICES

301. OPERATING SYSTEMS SERVICES

Operating System services are currently out of CITA scope. A brief rationale is given below. Further details can be found in CCEB Publication 1007.

302. RATIONALE FOR RULING SERVICES OUT OF SCOPE

This category encompasses the standards for services provided by computer operating systems and the means by which user applications access them. Operating Systems are relevant to the porting and reuse of applications software. It is recognised that they can contribute to interoperability in some circumstances (e.g. where an OS specific application is essential to achieve a common understanding of exchanged data). However, there is no general inter-nation requirement for porting and reuse at this time. It is anticipated that WIN32 or UNIX 95 standards would be specified if a CCEB requirement were to arise.

This page intentionally blank

CHAPTER 4

USER INTERFACE SERVICES

401. USER INTERFACE SERVICES

User Interface services are currently out of CITA scope. A brief rationale is given below. Further details can be found in CCEB Publication 1007.

402. RATIONALE FOR RULING SERVICES OUT OF SCOPE

This category covers standards relevant to the Human-Computer Interface, including look and feel standards/conventions, APIs for windowing systems, desktop managers plus desktop hardware and operating system environments. The majority of standards in this category contribute towards applications portability or people portability; they are not, therefore, relevant to CITA interoperability objectives.

The few standards that are relevant to interoperability such as remote presentation protocols (e.g. X11) and inter-process communication protocols (e.g. DCOM), are included in Chapter 0 on Distributed Computing.

This page intentionally blank

CHAPTER 5

NETWORK SERVICES

501. SERVICE AREA SCOPE

The Network Services category includes the following services:

a. Messaging services

b. Directory services

c. Naming and Addressing services

d. Remote terminal services

e. File Transfer services

f. ISO services on top of the transport layer

502. MESSAGING SERVICES

a. **Description of Service:** This service provides users with the means to create and transfer information in the form of messages to one or more recipients at local or remote locations. Messages are transferred in one or more store-and-forward hops.

b. **Scope of Service:** The CITA scope is limited to message transfer protocols and message content formats. Where attachments are to be exchanged, relevant data interchange standards also apply. Message security services are covered in Chapter 14.

Text-oriented and bit-oriented structured messages are covered in Chapter 9.

c. **Assessment of Scope:**

1. **Inter-Nation Requirement:** There is a clear inter-nation requirement.

2. **Openness:** Open solutions exist for server to server message transfer protocols (e.g. the X.400 P1 protocol).

3. **Boundary Issues:** Support is only required for message transfer protocols and message content formats. The CITA does not specify messaging protocols or formats used nationally. Agreement is also required on security profiles used at boundaries, including message labelling formats.

4. **Legacy Issues:** Support is required within the messaging infrastructure for ACP127 (Radio and Teletype RATT Broadcasts) and other legacy messaging protocols.

5. **Cost/Risk Issues:** Most COTS solutions do not satisfy all military requirements. However, systems which are designed specifically for military applications can result in higher developmental and life cycle costs due to the need to obtain additional maintenance support.

6. **Interconnection Security Issues:** Secure message gateways may be necessary to mediate security services between domains.

7. **System Evolution:** COTS functionality is converging with military requirements.

8. **Conclusion:** Only message transfer protocols and message content formats are within CITA scope. Where attachments are to be exchanged, relevant data interchange standards also apply. Security services for messaging are considered separately (Chapter 14).

d. **CITA Specification:**

1. **Organisational Messaging**:

Message transport submission & delivery (P1/P3/P7) ACP 123 Annex C.(with STANAG 4406 Alpha Profile Set profile AMH91 (MA), plus support for the file transfer body part).

Gateway between MMHS and ACP127 to be defined.

Content Type (P772, ACP 123 Annex A, Annex B, Annex D)

Message Store Attributes (P772, MS Attributes, ACP 123 Annex E, Annex F)

2. **Interpersonal Messaging:** There is presently no agreed requirements for interpersonal messaging. The CITA WG recommends SMTP (RFC 821) + MIME (RFC 2045) where used.

3. **Naming and addressing**:

ACP 133 for Directory Services;

ACP 123 for Messaging Services;

e. **CITA Evolution:** The existence of an agreed requirement for interpersonal email should be monitored.

503. DIRECTORY SERVICES

a. **Description of Service:** Services for the provision of information relating to all forms of communications and information services including the support messaging and security services.

b. **Scope of Service:** CITA scope covers CCEB. ACP 133 specifies a scaleable directory system in support of many forms of communication including, but not limited to, organisational communication (e.g. Postal), Telecommunications, Messaging, Secure Messaging, User Authentication and information relating to Task Force organisation and tactical (mobile) units (e.g. ships). The directory must support the public key infrastructure required by allied security policy.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a clear inter-nation requirement for an allied directory system that supports the transfer of directory information. This requires that the following are standardised (as per ACP 133):
   - access and interchange protocols;
   - common schema;
   - common security, authorisation and certificate policy.

   The directory will also be responsible for provision of security certificates which are demanded by the CCEB messaging profile.

2. **Openness:** Standards for directory systems exist (e.g. X.500,) and have growing product support.

3. **Boundary Issues:** Border directory systems will be used according to national policy to ensure that sensitive national directory information is protected from the shared environment. Strong Authentication will be used for client and server connections to provide the correct levels of trust in the access and transfer of directory information.

4. **Legacy Issues:** Generally directory systems have been applied to network level services or in a localised context for local messaging systems. Support is required between an ACP 133/X.500 and either an ACP 100/ACP 117 environment or a proprietary/Internet environment. These will require integration and consolidation with ACP 133/X.500 based systems in order to scale and provide the allied service levels demanded with the full range of security requirements.

5. **Cost/Risk Issues:** The risk to allied capability is that the directory support services are not provided in a secure and scaleable way. Since ACP 133 defines a target, nations may in the interim implement similar, yet non-interoperable subsets of the specification.

6. **Interconnection Security Policy:** As defined in ACP 133 and other ACPs that apply directory for security services.

7. **System Evolution:** There is a need to rationalise and manage directory information within nations to ensure consistent information is input into any allied system.

8. **Conclusion:** ACP 133 must be applied to provide the most effective and secure way of providing all forms of information and voice exchange between the allied nations.

d. **CITA Specification**

ACP133 (based on X.500 1992 with some 1997 extensions).

e. **CITA Evolution**

CITA WG will monitor developments in national directory service projects.

An SMTP E-mail addressing schema will need to be formulated as per ACP133.

504. NAMING AND ADDRESSING SERVICES

a. **Description of Service:** Services for the resolution of computer or server names into specific addresses.

b. **Scope of Service:** Services applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement for the exchange of naming and addressing data.

2. **Openness:** Open standards exist.

3. **Boundary Issues:** Different name services may be used nationally (e.g. WINS).

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Policy:** Automated exchange of naming information may be prohibited for some interconnections.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

DNS (RFC 1035), which is the Internet domain naming system.

For Messaging-specific naming and addressing services see section 502.

e. **CITA Evolution:**

A domain naming policy will have to be developed.

505. REMOTE TERMINAL SERVICES

a. **Description of Service:** Protocols and applications that enable remote terminals to connect into a system. They include both OSI application-layer standards and their Internet Protocol Suite (IPS) equivalents. Such connections typically emulate character-based terminals and are used to provide access to legacy systems.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** The requirement for remote terminal access between nations is limited to legacy systems.

2. **Openness:** IPS applications are open. OSI Protocol Suite (OSIPS) applications are less well supported.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** Remote terminal possibly the only means of interoperability with certain legacy systems.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Direct forms of interconnection, especially remote terminal, will often be precluded by security policy.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification**

TELNET (RFC 854/855) for remote terminal.

e. **CITA Evolution**

TELNET is expected to remain a current standard as long as there is a requirement to support connections to legacy systems.

506. FILE TRANSFER SERVICES

a. **Description of Service:** Protocols and applications to provide a file transfer facility. They include both OSI application-layer standards and their IPS equivalents.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA:**

1. **Inter-Nation Requirement:** There is a clear inter-nation requirement for file transfer.

2. **Openness:** IPS applications are open. OSIPS applications are less well supported.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Direct forms of interconnection will often be precluded by security policy.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

1. FTP (RFC 959) and HTTP v 1.1 for file transfer. For HTTP, this is in practice as implemented by Netscape and MS Explorer, and their interoperable proprietary extensions.

2. For file transfer in constrained environments it is recommended that FTP products be used that implement the 'Restart' elements of RFC 959.

e. **CITA Evolution:**

FTP and HTTP are expected to remain current standards for the foreseeable future. The applicability of Trivial FTP and Enhanced Trivial FTP needs to be monitored. The HTTP Distribution and Replication Protocol also needs to be monitored.

507. ISO SERVICES ON TOP OF THE TRANSPORT LAYER

a. **Description of Service:** Services and protocols at application, presentation and session layers that enable OSI applications (e.g. X.400) to operate over the Internet Protocol Suite.

b. **Scope of Service:** These are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements arise from:

   – those applications (e.g. OSI X.400) that make use of specific OSI upper layer protocols;

   – those distributed computing services that make use of, or independently provide, OSI upper layer functionality.

2. **Openness:** Not applicable.

3. **Boundary Issues:** Conformance to upper layer protocol standards is solely determined by CITA requirements in other areas (e.g. messaging, RPC).

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

RFC 1006.

e. **CITA Evolution:**

None at present.

CHAPTER 6

COMMUNICATIONS SERVICES

601. SERVICE AREA

This chapter specifies the standards that may be used when communications systems from CCEB Nations are interconnected to form an IP-based backbone infrastructure. Whereas the CCEB does not have a permanent infrastructure, systems are brought together to form a network, an example being the CWAN constructed for the JWID.

Services included in this area are:

a. Telephony (Secure & Insecure)

b. Wide Area Networks

c. Point-to-point

d. Tactical data links

e. Internetworking standards

f. Routers

g. Transport

h. SATCOM bearers

i. Radio bearers

j. Cable bearers.

602. INTERCONNECTION SECURITY ISSUES

Whenever systems interconnect, there is a significant impact on the security of systems. Widely interconnected systems will always provide opportunities for attack that are absent in a standalone system. In order to maintain an acceptable level of security, significant issues such as accreditation, International key management and cryptographic standards must be addressed.

How systems are interconnected will depend on the services that need to be supported and the level of trust between them. Within the context of the CITA it is anticipated that some kind of firewall or guard will be at the boundary of each system. The interconnection between systems could employ a

number of technologies (e.g. PPP, Ethernet, ATM etc.) *between* firewalls, i.e. it is unlikely that such connections would be allowed to bypass the firewall.

Virtual Private Networks (VPNs) can be created by encrypting the insecure links between systems. This is analogous to the way VPNs are created commercially using the Internet. Two remote (secure) LANs can be connected, via the Internet, to form a single VPN if the routers at the gateway of each LAN encrypt all traffic passed between them.

In the following paragraphs these issues are regarded as overarching all considerations, hence they are not repeated; any additional issues specific to a communications system type are separately identified.

603. TELEPHONY

a. **Description of Service:** Services for secure and insecure voice communications across both analogue and digital dial-up connections. Modem and communications compression services are also included. Voice encoding standards are covered in the Data Interchange chapter.

b. **Scope of Service:** Dial-up connections between any participants in CCEB joint operations.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement to link into national telephone networks of CCEB nations during joint operations. There is also a requirement for CCEB nations to communicate over secure telephone circuits.

2. **Openness:** Standards are available.

3. **Boundary Issues:** Secure telephony requires user equipment to conform to agreed standards, hence it is not purely a system boundary issue.

4. **Legacy Issues:** Not significant.

5. **Cost/Risk Issues:** Not significant.

6. **Interconnection Security Issues:** Secure telephony requires the use of accredited user equipment.

7. **System Evolution:** Not significant.

8. **Conclusion:** Telephony standards are within CITA scope. Specific communications compression standards (e.g. V.42) may need to be standardised within specific nations, or for use within the CCEB communications infrastructure.

d. **CITA Specification:**

1. For Secure telephony: STU-IIB compliant equipment.

2. For Insecure telephony: standards selected from ITU-T Recommendations, including:

   Series E - Overall network operation, telephone service, service operation and human factors;

   Series G - Transmission systems and media, digital systems and networks;

   Series P - Telephone transmission quality, telephone installations, local line networks;

   Series Q - Switching and signalling;

   Series V - Data communication over the telephone network.

3. V.34 for Modem standard.

4. V.42 for communications compression.

e. **CITA Evolution:**

1. The STU-IIB standard is soon to be replaced by STE (Secure Telephone Equipment).

2. Voice-over-IP standards are experiencing growing market take-up and should be monitored.

3. As the V.90 modem standard (56 Kbits/sec) becomes widely adopted, the CITA specification will be upgraded to this standard.

604. WIDE AREA NETWORKS

a. **Description of Service:** Services provided for the transfer of data across wide area networks including X.25, ISDN, B-ISDN(ATM) and SONET.

b. **Scope of Service:** Services are applicable to the interconnection level of interoperability. The CITA scope limited to the specification of the services provided by the wide-area communications infrastructure (i.e. data link and physical layer specifications at point of attachment). No use of an OSI network-layer protocol assumed.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a requirement for standardisation of the services provided by the wide-area communications infrastructure.

2. **Openness:** Open standards exist.

3. **Boundary Issues:** Unless interconnections are mediated by a gateway, interoperating end-systems must employ the same internetworking and transport protocol.

4. **Legacy Issues:** See system evolution.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No further issues.

7. **System Evolution:** Wide-area communications infrastructure evolves slowly because of the investment required for change. Wide-area networks will continue to offer services long after the corresponding standards have been superseded.

8. **Conclusion:** The CITA scope is limited to the specification of the services provided by the wide-area communications infrastructure (i.e. data link and physical layer specifications at point of attachment). The technologies used to implement the service are within CITA scope, but see conclusions under bearer systems.

d. **CITA Specification:**

X.25	X.25 support required for legacy networks into next century.
X.121 addressing policy	X.121 registrations required to support X.25.
ISDN	ITU-T Series I Recommendations.
B-ISDN (ATM)	ITU-T Series I Recommendations
	ATM Forum af-standards for physical and adaption layers.
	LAN Emulation (LANE) af-0087.000 v2.0.
SONET/SDH[8]	ANSI T1.105.

[8] SDH is the ITU-T standard for packaging cells over fibre-optic bearers at data rates of greater than or equal to 155.52 Mbit/s. SDH is a physical layer technology capable of being used with systems supporting a variety of protocol stacks and providing a path for unlimited upgrades at intervals of 51.8 Mbit/s up to a maximum of 10 Gbit/s. SONET is the North American standard equivalent to SDH which provides data rates starting at 51.8

The CITA would prefer to specify a single standard, however member nations have each made significant investment in a number of standards. For this reason all relevant standards are listed here.

e. **CITA Evolution:**

It is the CITA view that ATM will eventually emerge as the preferred single standard.

605. POINT-TO-POINT SERVICES

a. **Description of Service:** Services providing full duplex, synchronous or asynchronous network connections over a serial line.

b. **Scope of Service:** Services are applicable to point-to-point communications.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement.

2. **Openness:** Open Internet standards are in common use.

3. **Boundary Issues:** Not significant.

4. **Legacy Issues:** Not significant.

5. **Cost/Risk Issues:** Not significant.

6. **Interconnection Security Issues:** No further issues.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Point-to-point protocols are within CITA scope.

d. **CITA Specification:** RFC 1661/1662 (PPP);

RFC 1332 (PPP Internet Protocol Control Protocol);

RFC 1989 (PPP Link Quality Monitoring);

Mbit/s and increasing by multiples of 51.8 Mbit/s. Whilst SONET and SDH have many similarities, there are some important differences relating to data rates and multiplexing strategies which may prevent interoperability. SDH Networks can only interoperate successfully with SONET networks if appropriate data rates and multiplexing strategies are selected.

ACP 140

RFC 1994 (PPP Challenge Handshake Authentication (CHAP));

RFC 1570 (Link Control Protocol (LCP) Extensions).

e. **CITA Evolution:**

None at present.

606. TACTICAL DATA LINK SERVICES

a. **Description of Service:** Tactical data links provide the means for exchanging tactical information used for battle management.

b. **Scope of Service:** Tactical systems requiring interconnection.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement for tactical data links to be available during combined operations.

2. **Openness:** Defence standards exist.

3. **Boundary Issues:** Internal tactical data links are outside CITA scope.

4. **Legacy Issues:** Not significant.

5. **Cost/Risk Issues:** Not significant.

6. **Interconnection Security Issues:** No further issues.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Tactical data links are within CITA scope. Link 11 is widely used throughout NATO with air and naval forces.

d. **CITA Specification:**

1. Link 11

STANAG 5511 annex B, Radio performance & protocols; vol.2, Link 11B Waveform protocol changes.

MIL-STD-118-2031a, Conventional Link 11 Waveform 16 tones.

SPAWAR-5-850, Single tone Link 11 Waveform

2. Link 16

   STANAG 4175 edition 1

3. Link 22

   UHF STANAG 4372 (Saturn); Saturn can also carry Link 11 and Link 16 messages.

   HF STANAG 4444 (Slow hop ECCM)

4. Link forwarding STANAG 5616.

e. **CITA Evolution:**

The use of Variable Message Format (VMF) should be monitored.

607. INTERNETWORKING STANDARDS

a. **Description of Service:** Standards for the transfer of data across LAN/WAN and LAN/LAN boundaries.

b. **Scope of Service:** Limited to the specification of the permissible modes of LAN/WAN and LAN/LAN interworking for the purposes of interconnection.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement as part of a CCEB communications infrastructure.

2. **Openness:** Open standards are in common use.

3. **Boundary Issues:** Not significant.

4. **Legacy Issues:** Not significant.

5. **Cost/Risk Issues:** Not significant.

6. **Interconnection Security Issues:** The development and deployment of strong IP level encryption devices will significantly improve the CCEB's ability to construct a secure IP backbone network..

7. **System Evolution:** No impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

IPv4 (RFC 791). Awaiting CCEB policy on IP addressing.

e. **CITA Evolution:**

IPv6 (RFC 1883).

608. TRANSPORT SERVICES

a. **Description of Service:**

Services providing user access to internetworking services and end-to-end quality enhancement.

b. **Scope of Service:** Services are applicable to the interconnection level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Openness:** Open standards exist.

2. **Boundary Issues:** No significant impact.

3. **Legacy Issues:** No significant impact.

4. **Cost/Risk Issues:** No significant impact.

5. **Interconnection Security Policy:** No significant impact.

6. **System Evolution:** No significant impact.

7. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

TCP (RFC 793); UDP (RFC 768).

No use of OSI transport-layer protocol assumed.

e. **CITA Evolution:**

None at present.

609. ROUTERS

a. **Description of Service:** Routers are COTS products used to interconnect networks of differing types or different domains, including sub-networks and end systems.

b. **Scope of Service:** Services are applicable to network interconnection.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement to link national networks.

2. **Openness:** Open standards are available.

3. **Boundary Issues:** Bridging Routers frequently form the boundary between networks. They will, therefore form the focus for many of the interoperability standards.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Routers are often used to provide screening, encryption and other security functions.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Routers are within CITA scope.

d. **CITA Specification:**

RFC 1812 (Requirements for IPv4 routers). Routers shall use Border Gateway Protocol 4 (BGP-4) for exterior gateway routing.

e. **CITA Evolution:**

Move to standards associated with IPv6 - Transition Mechanisms for IPv6 Hosts and Routers (RFC 1933).

610. SATCOM BEARERS

a. **Description of Service:** Standards for the transfer of data across SATCOM links including UHF, SHF, and EHF.

b. **Scope of Service:** Services are applicable to satellite communications.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement for satellite communications using national, international and commercial facilities.

2. **Openness:** There are recognised MIL-STDs and STANAGs applicable to SATCOM bearers.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No further issues.

7. **System Evolution:** No significant impact.

8. **Conclusion:** SATCOM bearers are within CITA scope.

d. **CITA Specification:**

1. **General**

(a) MIL-STD-188-146 Interoperability And Performance Standards For Satellite Communications, 15 June 1998

Note: ABCA information on SATCOM capabilities is given in QAP 142.

2. **UHF**

(a) MIL-STD-188-181A, Interoperability Standard for Single Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 31 March 1997.

(b) MIL-STD-188-182A, Interoperability Standard for 5-kHz UHF DAMA Terminal Waveform, 31 March 1997.

(c) MIL-STD-188-183, Interoperability Standard for 25-kHz UHF/TDMA/DAMA Terminal Waveform, 18 September 1992; with Notice of Change 1, 2 December 1996 (STANAG 4231).

(d) MIL-STD-188-184, Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993.

(e) MIL-STD-188-185, DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996.

3. **SHF**

(a) MIL-STD-188-164, Interoperability and Performance Standards for C-Band, X-Band, and Ku-Band SHF Satellite Communications Earth Terminals, 13 January 1995.

(b) MIL-STD-188-165, Interoperability and Performance Standards for SHF Satellite Communications PSK Modems (Frequency Division Multiple Access (FDMA) Operations), 13 January 1995.

4. **EHF**

(a) MIL-STD-1582D, EHF LDR (Low Data Rate) Uplinks and Downlinks, 30 September 1996; with Notice of Change 1, 14 February 1997 (STANAG 4233).

(b) MIL-STD-188-136, EHF MDR (Medium Data Rate) Uplinks and Downlinks, 26 August 1995; with Notice of Change 1, 15 August 1996, and Notice of Change 2, 14 February 1997 (STANAG 4522).

e. **CITA Evolution:**

None at present.

611. RADIO BEARERS

a. **Description of Service:** Standards for the transfer of data across Radio links including VLF, LF, HF, VHF, UHF, and SHF. Combat Net Radio is also included.

b. **Scope of Service:** All systems requiring the interconnection level of interoperability through radio links.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No inter-nation requirement other than at point of attachment to wide-area communications infrastructure.

2. **Openness:** Established QSTAGS, MIL-STDs and STANAGs are available.

3. **Boundary Issues:** Standardisation is required only at the boundary.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Link level encryption will generally be required across radio bearers.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope in as far as it is necessary to capture the standards that could exist for radio bearer systems across the interconnection infrastructure.

d. **CITA Specification:**

1. **LF/VLF**

MIL STD 188-140A, Equipment Technical Design Standards for Common Long Haul/Tactical Radio Communications in the LF Band and Lower Frequency Bands, 1 May 1990.

2. **HF**

MIL STD 188-141A , Interoperability and Performance Standards for Medium and High Frequency Radio Equipment Standard, 15 September 1988; with Notice of Change 1, 17 June 1992, and Notice of Change 2, 10 September 1993.

STANAG 4203 Technical standard for single channel HF radio equipment.

3. **VHF**

MIL STD 188-242, Tactical Single Channel (VHF) Radio Equipment, 20 June 1985.

STANAG 4204 Technical standard for single channel VHF radio equipment.

4. **UHF**

MIL STD 188-243, Tactical Single Channel (UHF) Radio Communications, 15 March 1989.

STANAG 4205 Technical standard for single channel UHF radio equipment.

5. **SHF**

MIL STD 188-145, Digital Line-of-Sight (LOS) Microwave Radio Equipment, 7 May 1987; with Notice of Change 1, 28 July 1992.

6. **CNR (Voice only)**

CNRs are interoperable for fixed frequency (VHF) voice communications only. There are no commonly agreed standards for frequency agility. The standards are:

QSTAG 734 (STANAG 4204) Technical Standards for Single Channel VHF Radio Equipment.

QSTAG 1108 (STANAG 4197A) Common Critical Crypto Standards for Single Channel Communications (Voice, Teletype and Data) for VHF CNR.

7. **Data modems**

MIL-STD-188-110A Interoperability and Performance Standards for Data Modems, 30 September 1991.

STANAG 4285 Characteristics of single tone modems for HF radio.

e. **CITA Evolution:**

Standards for the Joint Tactical Radio (JTR) need to be monitored.

612. CABLE BEARERS

a. **Description of Service:** Standards for the transfer of data across copper and fibre links including Optical, Shielded Twisted Pair (STP), and Unshielded Twisted Pair (UTP).

b. **Scope of Service:** Services are applicable to physical interconnection.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No inter-nation requirement other than at point of attachment to wide-area communications infrastructure.

2. **Openness:** Open standards exist.

3. **Boundary Issues:** Standardisation is required only at the boundary.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No further issues.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope in as far as it is necessary to capture the standards for physical bearer systems that could exist across the interconnection infrastructure.

d. **CITA Specification:**

RS-232;

RS-422; RS-423; RS-530;

EIA - 4920000A;

EIA - 5090000.

e. **CITA Evolution:**

None at present.

CHAPTER 7

DISTRIBUTED COMPUTING

701. SERVICE AREA

Services included in this area are:

a. Distributed database management services

b. Distributed Process (RPC)

c. Remote presentation services

d. Distributed file services

e. Distributed time services

f. Distributed print services

g. Distributed transaction processing services

h. Distributed object services (Object middleware)

i. Distributed system management services

There are a number of competing standards for distributed computing. All are emerging and there is no clear leader at present. Most use remote procedure call (RPC) mechanisms to effect distribution of computational effort, the exception being Java. The main contenders are:

Active X: this is Microsoft's standard based on its Distributed Component Object Model (DCOM) technology. It is being ported to most UNIX platforms.

CORBA: Common Object Request Broker Architecture is the Object Management Groups (OMG) attempt to introduce open standards into distributed computing. The OMG is a consortium of companies developing these standards but relying on individual companies to provide products.

DCE: Distributed Computing Environment is the Open Group's standard for distributed computing.

JAVA: Sun's attempt to produce truly portable programs has been taken up by a number of vendors. It uses a Java Virtual Machine (JVM) to execute Java code. Any platforms that support a JVM should (in theory) be able to execute any Java program. Java programs can be distributed (and

executed) across a federation of computing platforms. It should be noted that practice and theory have not fully converged.

702. DISTRIBUTED DATABASE MANAGEMENT SERVICES.

a. **Description of Service:** This section covers services for maintenance of databases distributed over multiple physical locations. They are listed and addressed under Nation-level data management paragraph 804 .

703. DISTRIBUTED PROCESS (RPC).

a. **Description of Service:** Remote procedure call (included in this category are the other forms of inter-process communication).

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is no evidence of an inter-nation requirement but future requirements may arise.

2. **Openness:** Sufficiently open standards exist at present. A number of standards exist namely ONC+ RPC, DCE RPC and Windows RPC; all interoperable to an extent but not in a secure manner.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** System security policy may preclude the direct interconnection between systems demanded for RPC.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope at present. Possible requirements and status of standards and products need to be monitored.

d. **CITA Specification**

None.

e. **CITA Evolution**

Emergence of requirements for use of RPC needs monitoring. CORBA IORPC, ONC+ RPC, DCE RPC and Active X are all interoperable to an extent but not in a secure manner. Therefore future inclusion dependent also upon inclusion of relevant security services. Acceptably open standards may emerge but cannot yet be identified.

704. REMOTE PRESENTATION SERVICES.

a. **Description of Service:** These are protocols permitting graphical user interfaces to execute remotely from the client application (e.g. X11, Windows NT Terminal Server (Hydra), Citrix WinFrame/MetaFrame).

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No evidence of an inter-nation requirement.

2. **Openness:** Open standards exist for UNIX environment (X11). Widely licensed, proprietary standards exist for the Windows environment.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope because there is no evidence of an inter-nation requirement. (For other graphics services see Data Interchange.)

d. **CITA Specification:** None.

e. **CITA Evolution:**

The ability of a user to render a remote application’s GUI display on a local workstation may become a future a requirement. Technology has existed for some time that enables users to render UNIX displays on NT workstations. Technology to allow the rendering of NT displays on UNIX workstations has existed but not been part of main stream developments. More

recently, however, the appearance of Windows NT Terminal Server Edition (Hydra) has brought such technology into a main stream product. Further, these services are planned to be available in Windows 2000 (i.e. NT v5).

705. DISTRIBUTED FILE SERVICES.

a. **Description of Service:** File sharing protocols.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No evidence of an inter-nation requirement.

2. **Openness:** Open standards exist (e.g. SMB, NFS).

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Policy:** File services are usually at the heart of a system security policy. File sharing between systems may therefore force systems to adopt uniform security policies.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope because there is no inter-nation requirement. If an inter-nation requirement emerges then this service would come into scope. Security constraints would still be an issue.

d. **CITA Specification:** None.

e. **CITA Evolution:** None.

706. DISTRIBUTED TIME SERVICES.

a. **Description of Service:** These are protocols for synchronisation of system clocks.

b. **Scope of Service:** Services applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No evidence of an inter-nation requirement, however see conclusion below. Also, it is important that systems handle time consistently, particularly with regard to Y2K.

2. **Openness:** Open standards exist (e.g. NTP).

3. **Boundary Issues:** Different time protocols may be used internally (e.g. Microsoft proprietary).

4. **Legacy Issues:** No significant impact with respect to time synchronisation, however see conclusion (below) regarding Y2K.

5. **Cost/Risk Issues:** No significant impact with respect to time synchronisation, however see conclusion (below) regarding Y2K.

6. **Interconnection Security Issues:** System time is relevant to several system security functions (e.g. auditing) so many system security policies will preclude remote synchronisation, but see conclusion below.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope because there is no inter-nation requirement. However, the Common Security Protocol (CSP) detailed in ACP 120 identifies a number of security services that require a time stamping service. Also the need to synchronise X.500 directories across nations (because of Certificate Revocation Lists) may require a time synchronisation protocol. The CMI WG and AIS ISME will provide necessary advice.

   Time issues regarding Y2K are relevant to interoperability in so far as it is necessary for end-systems to correctly interpret time information. Individual nations will normally be required to ensure that systems within their control are Y2K compliant. This may involve considerable cost and risk, particularly where legacy systems are involved.

d. **CITA Specification:** None.

e. **CITA Evolution:**

If a requirement is forthcoming then NTP V2 (Network Time Protocol Version 2) RFC 1119 would be the recommended standard. NTP V3 (RFC 1305) is currently a draft standard. Also, to support the security services, the use of UTC and Generalised Time should be included.

707. DISTRIBUTED PRINT SERVICES.

a. **Description of Service:** Protocols for transfer of print jobs from client to spooler/printer.

b. **Scope of Service:** All required for the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No evidence of an inter-nation requirement.

2. **Openness:** Open standards exist (e.g. SMB, LPD).

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Procedural aspects of control over printed output may limit the distribution of print jobs between systems.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope because there is no evidence of an inter-nation requirement.

d. **CITA Specification:** None.

e. **CITA Evolution:** None.

708. DISTRIBUTED TRANSACTION PROCESSING SERVICES.

a. **Description of Service:** These are services for the management of transactions involving participants on different end-systems.

b. **Scope of Service:** Services applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No evidence of an inter-nation requirement but future requirements may arise.

2. **Openness:** No open standards.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope at present primarily because there is no evidence for a requirement at this time. Future requirements and the status of standards and products will be monitored.

d. **CITA Specification:** None.

e. **CITA Evolution:** None.

709. OBJECT INTERCHANGE STANDARDS.

a. **Description of Service:** Data formats relevant to the encoding of object structures used in distributed computing. The specific formats cited are OLE and OpenDoc. These services are also listed in the distributed computing category.

b. **Scope of Service:** Standards are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements in this area include the representation of objects embedded within OA documents and the exchange of objects between nations' systems.

2. **Openness:** Sufficiently open standards (e.g. CORBA & DCOM) exist.

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** CORBA and DCOM use RPCs, for which no acceptably open security standard exists. Therefore it will not be possible to use such mechanisms in situations where access controls need to be applied.

7. **System Evolution:** No significant impact.

8. **Conclusion:** OA document formats are covered under Document Interchange Standards, paragraph 902.

d. **CITA Specification:**

CORBA/IIOP v 2.2; DCOM.

e. **CITA Evolution:** The range of standards needed may broaden in the medium term with the increasing trend towards executable content in Internet technologies. Although it is not possible at present to predict which standards are likely to dominate, the modelling and simulation high level architectures warrant particular attention. Monitoring is required.

710. DISTRIBUTED OBJECT SERVICES (OBJECT MIDDLEWARE).

a. **Description of Service:** These are **s**ervices for location of, or access to, objects when distributed over a network.

b. **Scope of Service:** Services applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No evidence of an inter-nation requirement but future requirements may arise.

2. **Openness:** Sufficiently open standards exist.

3. **Boundary Issues:** Competing standards are interoperable to a degree.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Risks associated with import of logic bombs or viruses are greatly magnified with distributed object technologies making interconnection impractical for many systems at present.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope at present primarily because there is no evidence for a requirement at this time. Possible requirements and status of standards and products need to be monitored.

d. **CITA Specification:** None.

e. **CITA Evolution:** Evidence of a requirement for use of RPC across nation boundaries needs confirmation. Acceptably open standards (e.g. CORBA and DCOM) have emerged and there is some cross-platform support. However, it is unlikely that security considerations will permit distributed object services to be employed widely in the foreseeable future. Also, Middleware may not feature in all individual nation's technical architectures.

711. DISTRIBUTED SYSTEM MANAGEMENT SERVICES.

a. **Description of Service:** Services for the co-ordinated management of various distributed components within a system.

b. **Scope of Service:** Services applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No evidence of an inter-nation requirement.

2. **Openness:** No open standards.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** System management requires high access rights (e.g. Root/Administrator passwords).

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope because there is no evidence of an inter-nation requirement. System management functions such as creating user accounts, installing applications, configuring servers and managing file stores, frequently require high system access rights or 'superuser' privileges. System security boundaries (e.g. firewalls) will prevent system management protocols from passing through them.

d. **CITA Specification:** None.

e. **CITA Evolution:**

If a coalition or combined Intranet has to be managed on a long-term basis, it would be desirable if the management functions could be performed using suitable standards and tools, assuming security requirements could be met. The management of the CWAN is described in paragraph 1005.

CHAPTER 8

DATA MANAGEMENT SERVICES

801. SERVICE AREA

Services included in this area are:

a. Remote data access

b. CCEB-level data management

c. Nation-level data management

1. Data dictionary services

2. Database management system services

3. Database replication

802. REMOTE DATA ACCESS.

a. **Description of Service:** These are mechanisms that allow client terminals to access data on a remote database server in a client/server environment.

b. **Scope of Service:** Services applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement for remote data access (e.g. between server/server environments).

2. **Openness:** No open standards for remote data access protocols although some (e.g. SQL*NET (ORACLE) and ODBC) are regarded as sufficiently open being dominant products.

3. **Boundary Issues:** Interworking/middleware products exist which could offer a defined interface at system boundary but these presently offer only limited functionality.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Interconnection security policy will often prohibit direct client/server access between nations.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope because there is an inter-nation requirement for remote data access (but between server environments). Emergence of future Internet standards will need to be monitored.

d. **CITA Specification:**

ODBC v 2.

Microsoft's ODBC has cross-platform support and is favoured over any of the proprietary versions of SQL. ODBC provides a consistent interface between itself and an application; it generates vendor-specific SQL at its interface with a database product.

It is questionable whether, in practice, a client terminal on one nation's CIS system accessing data on another nation's server would be used (or permitted). It is more likely that a server-to-server transaction would be used.

e. **CITA Evolution:**

ODBC v3 is currently emerging as is JDBC (Java DBC); both should be monitored. HTTP-based access protocols are currently used across the Internet; presently they offer only very limited database functionality but should also be monitored.

803. CCEB-LEVEL DATA MANAGEMENT.

a. **Description of Service:** This category covers what would normally be described as data management. It includes data models plus associated metadata standards and data management procedures.

b. **Scope of Service:** Services applicable to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Interoperability requires common syntactic and semantic understanding of data. This necessitates standardisation of data definitions and schema. However, from a CITA perspective:

- only data exchanged between systems needs to be standardised;

- only data common to all, or most, nations needs to be standardised in the CITA.

Both categories are impossible to predict fully and accurately in advance.

2. **Openness:** Metadata standards are open but there are no open standards for military data (except geospatial and hydrographic; see standard data products).

3. **Boundary Issues:** For interoperability purposes standardisation can be limited to external schema. Current work presupposes a relational database-to-database method of interoperability. Object approaches providing encapsulation may permit standardisation to be limited to methods provided at system boundaries.

4. **Legacy Issues:** Much existing software uses well established military data models.

5. **Cost/Risk Issues:** Widespread data standardisation requires huge investment. Bilateral arrangements are likely to be cheaper in some circumstances.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** Common data definitions obviate the need to update many local data definitions as individual systems evolve or are adapted to meet new requirements.

8. **Conclusion:** Within CITA scope. The unpredictability of future operations and the need for flexibility to meet unforeseen interchange requirements emphasises importance of CCEB-wide rather than local agreements. However, priority for CITA data standardisation efforts should, at least initially, be on those items where there is firm evidence of a current or likely future CCEB-wide requirement for exchange of that data. CCEB policy needs to recognise the possible emerging role of object-based approaches. Within CCEB the best that can at present be practically achieved is to define a common logical data model that each nation can map on to.

d. **CITA Specification:**

Current definition should, where possible, focus on those data items for which there is clear evidence of an inter-nation exchange requirement. These definitions should be maintained in a central repository to aid ready access and conflict resolution.

e. **CITA Evolution:**

Current CCEB policy is for data schema, syntax and semantics to be defined on a pan CCEB-basis. Newly emerging CCEB policy indicates that data management policy should

concentrate on defining the top 100 data items. Any CITA recommendation must reflect consequent changes in policy of individual CCEB nations.

A specific policy for database key management will be needed as part of overall policy for CCEB-level data management.

804 NATION-LEVEL DATA MANAGEMENT

804.1 DATA DICTIONARY SERVICES.

a. **Description of Service:** These are software tools that facilitate the development, management and use of nation-specific data dictionaries. They are not relevant to inter-nation interoperability and hence outside of the CITA scope; they are relevant to other objectives such as application portability or software reuse.

b. **CITA Specification:** None.

c. **CITA Evolution:** None.

804.2 DATABASE MANAGEMENT SYSTEM SERVICES.

a. **Description of Service:** These are the facilities provided by a conventional RDBMS. They are not relevant to inter-nation interoperability and hence outside of the CITA scope. They are relevant to other objectives such as application portability or software reuse.

b. **CITA Specification:** None.

c. **CITA Evolution:** None.

804.3 DATABASE REPLICATION.

a. **Description of Service:** These are mechanisms for replication of data between DBMSs, such as provided by modern commercial DBMS products.

b. **Scope of Service:** Services applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a requirement to support database replication by ‘push’ only. There are some aspirations to use database replication as a mechanism

to satisfy inter-nation interoperability requirements, although the extent of the requirement is unclear.

Replication may be employed within individual systems to meet survivability and performance requirements - this does not justify inclusion of this service within the CITA.

2. **Openness:** There are no acceptably open standards for replication protocols.

3. **Boundary Issues:** It is generally not feasible to convert between replication protocols at system boundaries, so a common protocol needs to be supported by interoperating database products. This would effectively force interoperating systems to use identical products.

4. **Legacy Issues:** Many legacy systems employ flat-file databases which do not support efficient replication protocols.

5. **Cost/Risk Issues:** Adoption of a single database product CCEB-wide will not be acceptable on procurement grounds.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope because of openness principle.

d. **CITA Specification:** None.

e. **CITA Evolution:**

Monitoring is required of the scale of the CCEB-wide requirement to determine if adoption of a bespoke solution is justifiable (and whether such a solution is likely to emerge from current initiatives). Any decision will also depend upon progress made in this area by NATO. The ATCISS product claims to provide the necessary functionality, however this has not been substantiated.

This page intentionally blank

CHAPTER 9

DATA INTERCHANGE

901. SERVICE AREA

Services included in this area are:

a. Document interchange standards

   1. Office Automation interchange formats

   2. Hypertext interchange formats

   3. Hypertext transfer protocols

b. Business-transaction-oriented data interchange standards

c. Military data interchange formats

d. Character sets and alphabets

e. Encoding standards

   1. Data

   2. Voice

f. Fax (Secure & Non-secure)

g. Video Conferencing

h. Distributed computing standards

i. Graphical/Still image data interchange standards

j. Standard Data Products/Geospatially referenced data interchange standards

k. Moving image and audio/visual data interchange standards

l. Audio data interchange standards

m. Data compression standards

1. General purpose file compression

2. Communications data compression

n. Multimedia and distributed real time service data interchange standards

o. Page description

p. Miscellaneous data interchange standards

902. DOCUMENT INTERCHANGE STANDARDS.

There are a multitude of different document interchange formats. For the purposes of this analysis, document interchange formats have been divided into two categories, Office Automation and hypertext. This category also includes HTTP, the hypertext transfer protocol. This section identifies only the interchange standard and not the version of type of OA tool employed.

902.1 OFFICE AUTOMATION INTERCHANGE FORMATS.

a. **Description of Service:** These are formats used for the interchange of documents between Office Automation (OA) tools (i.e. word processor, spreadsheet, etc.).

b. **Scope of Service:** Services applicable to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a CCEB-wide requirement to exchange OA documents.

2. **Openness:** MS Office formats are open by virtue of market dominance. De jure document formats (e.g. Open Document Architecture (ODA)) are not sufficiently well supported to qualify as acceptably open.

3. **Boundary Issues:** Support required for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** Many legacy OA packages are in use but functionally limited converters are available for many formats.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** The transfer of documents containing executable code (e.g. macros) could pose a security risk.

7. **System Evolution:** Concurrent support for different generations of interchange format required.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

1. Primary Standard

MS Office 95 interchange formats (Word v7, Excel v7, PowerPoint v7, Access v7)

2. Secondary Standard(s)

Rich Text Format (RTF);

Portable Document Format (PDF).

The MS Office OA suite is likely to remain the dominant product in the medium-term, hence its inclusion in the CITA as the primary interchange format. Any successful competing OA package would need to provide ready migration and thus would need to support MS Office formats for several years. Several legacy OA packages are in current use but functionally limited converters are available for most formats.

Rich Text Format (RTF) is a neutral document formatting language that is sometimes used to transfer word processing documents between heterogeneous WP systems, preserving much of the original format. Although RTF is proprietary to Microsoft, it is widely available and supported by products. Variations exist in the implementation of the standard by vendors thus limiting the usefulness of the standard.

RTF documents are typically much smaller than their Word equivalents, making it more suitable for use over low bandwidth connections; zip compression will further reduce the overall size of most documents.

Portable Document Format (PDF) is an Adobe proprietary standard. The free availability of readers (Acrobat) and the level of cross platform support make this a suitable candidate for inclusion in the CITA as secondary standard.

e. **CITA Evolution:**

MS Office 97 interchange formats.

MS Office 97 is already emerging as a replacement for MS Office 95, and is likely to supersede it in the medium term. Therefore MSO 97 format is identified as the emerging standard.

902.2 HYPERTEXT INTERCHANGE FORMATS.

a. **Description of Service:** These are formats for representation and transfer of hypertext documents.

b. **Scope of Service:** Services applicable to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a CCEB-wide requirement to exchange hypertext documents (for Intranet purposes or as an alternative interchange format of OA).

2. **Openness:** Open formats exist (HTML plus widely supported proprietary extensions).

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** Hypertext document standards are evolving rapidly but new versions are generally backwards compatible.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

1. Primary Standard

HTML v4.0 (Dynamic HTML)

Several browser products support this HTML standard. The recognised market leaders are Netscape Navigator v4 and MS Internet Explorer v4.

2. Secondary Standard(s)

SGML for high value, complex documents;

XML (eXtensible Markup Language) where meta-language data definitions are required.

e. **CITA Evolution:**

XML is a standardised text format conforming to ISO 8879, specifically designed for transmitting structured data to Web applications. It addresses the needs of Web publishers who encounter the limitations of HTML to express structured data. It simplifies SGML constructs for electronic delivery of documents and allows structured documents without the full complexity of SGML. Some Web browsers already support XML. It is anticipated that XML will eventually replace HTML as the dominant standard.

An approved standard for executable content may be required in medium term (e.g. Java). Monitoring is required.

902.3 HYPERTEXT TRANSFER PROTOCOLS.

a. **Description of Service:** Protocols used for the transfer of hypertext documents between systems, including selective transfer for 'browsing'.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a CCEB-wide requirement to transfer hypertext documents (for Intranet purposes).

2. **Openness:** Open protocols exist (HTTP).

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** HTTP only includes basic authentication. It therefore cannot be used in situations where access controls need to be applied on the basis of subscriber identity.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

HTTP v1.1.

e. **CITA Evolution:**

HTTP with Distribution and Replication Protocol supports the transfer of file differences (deltas) significantly reducing bandwidth consumption. It is reliant upon the use of XML for metadata definitions.

HTTP (v2.0), plus executable content-specific protocols in mainstream use at the time. Monitoring is required.

903. BUSINESS-TRANSACTION-ORIENTED DATA INTERCHANGE STANDARDS.

a. **Description of Service:** These are text- or bit-oriented formats for structured representation of business-related data.

b. **Scope of Service:** Services are applicable to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement for these interchange formats. Certain message formats are specific to a particular business function, so the strength of the CCEB-wide requirement for these is questionable.

2. **Openness:** Effective standards (either military-specific de jure standards or open commercial specifications) exist in most areas.

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** Some widely-used message formats vital for continued interoperability with legacy systems.

5. **Cost/Risk Issues:** See security issues below.

6. **Interconnection Security Issues:** There could be significant security issues regarding the use of digital signatures with EDI. This could entail significant cost and risk.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope (limited to those areas where CCEB-wide requirements exist).

d. **CITA Specification:**

STEP/ISO 10303 for product data;

UN/EDIFACT/ISO 9735 for EDI.

e. **CITA Evolution:**

The Standard for the Exchange of Product data (STEP), which underpins much of CALS, may ultimately govern much of the information flow with the procurement, management and maintenance of Defence equipment. The use of standards for specific types of CIS is likely to increase (e.g. in Command, Control and Intelligence systems (C2I), and Electronic Data Interchange (EDI) areas) but not all of these are relevant to CITA.

904. MILITARY DATA INTERCHANGE STANDARDS.

a. **Description of Service:** Encodings of military-specific information in structured or unstructured form. Structured formats include both binary (bit-level) encodings and text-based (machine and human-readable) messages.

Business-transaction-oriented data interchange standards do not presently include a number of relevant military message formats so these have been included here as an additional category.

b. **Scope of Service:** Services are applicable to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** All formats identified thus far are specific to C2I systems. (This category does not cover formats related to message handling policy (e.g.P772) which are covered separately below). C2I-specific messages can be included as the ‘body-part’ of ACP 123 messages.

2. **Openness:** These formats are military-specific but most are effective in the sense that they are widely supported.

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** The continuing support for the majority of these formats is required for legacy systems.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

STANAG 5511 (Link 11 standard);

STANAG 5516 (Link 16 standard);

STANAG 5522 (Link 22 standard);

OTH-Gold;

ADatP3 (STANAG 5500). There is an aspiration to employ ADatP3 messages for some inter-nation transfers as interconnections become more widespread.

e. **CITA Evolution:**

Moves towards the use of VMF need to be monitored.

905. CHARACTER SETS AND ALPHABETS.

a. **Description of Service:** Binary encodings used to represent alphanumeric characters and special characters used in foreign languages or technical literature.

b. **Scope of Service:** Services applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a CCEB-wide requirement to support a common character set.

2. **Openness:** International Alphabet #5 (with National variants) is the only genuinely open standard at present. Future product support for internationalised character sets (e.g. UNICODE) will become more widespread. IA#5 assumed by other formats (e.g. for OA).

3. **Boundary Issues:** Support required for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

International Alphabet (ITA) 5 (ASCII).

Currency identification characters are nation-specific, hence all currency values should be represented by their 3 letter ISO standard codes.

e. **CITA Evolution:** Monitoring of emergence of acceptably open standards for internationalised character sets required.

Internationalised character sets (e.g. UNICODE) are not yet sufficiently widely adopted to allow their use to be mandated in the current CITA. Such codes should become widely supported and acceptably open in the medium-term, but it is not yet possible to predict which of the potential internationalised codes will dominate.

906. ENCODING STANDARDS.

a. **Description of Service:**

1. **Data Encoding Standards:** These are standards for encoding of binary or structured data, usually for transfer via a communications medium. This category covers ASN.1 and its encoding rules and UUENCODE.

2. **Voice Encoding Standards:** These are standards used in telephony for the encoding of digitised voice.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement to exchange encoded data.

2. **Openness:** Many open encoding standards exist.

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

1. **Data Encoding Standards**

UUENCODE;

MIME; SMIME;

zip.

This category covers ASN.1 and its encoding rules, BinHex, Base64 etc. UUENCODE converts 8-bit to 7-bit binaries for mail transfer but this function is being superseded by MIME. It is likely that, for many systems, several additional encoding standards will be needed to provide for interoperability with legacy systems. The legacy systems themselves will dictate where and which standards are required.

2. **Voice Encoding Standards**

ALAW; μLAW (MU-LAW); CELP;

ALAW is a method of companding (or compressing) digitised voice; it is used in Europe and much of the world. μLAW is an alternate method that is used in the United States, Canada and Japan.

CELP is a voice coding standard widely used by the military for voice communications over low bandwidth (e.g. 4.8K baud) bearers.

e. **CITA Evolution:** As for current CITA. Other encoding standards may be standardised in the context of the interworking services that make use of them (e.g. x.400 or MIME with the standard content encoding types for mail).

907. FAX.

a. **Description of Service:** These are standards for representation and transfer of page images across both secure and insecure dial-up circuits.

b. **Scope of Service:** These Fax standards are only relevant to communications systems and are therefore applicable to the interconnection level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement to exchange fax data.

2. **Openness:** Open standards exist.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Special circuits and user equipment is required for secure fax transmission.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope. Fax transmission standards are relevant to the communications systems only.

d. **CITA Specification:**

1. **Secure Fax**

STU-IIB compliant equipment.

2. **Insecure Fax**

Group 3 and Group 4;

The ITU-T Recommendations for Facsimile Standards (Recommendation T.4 (1992) -*Standardisation of Group 3 Facsimile Apparatus for Document Transmission* and Recommendation T.6 (1992) - *Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus*) define encoding schemes for black-and-white raster images.

Group 3 Fax is now the most widely used fax standard in the world. A Group 3 Body Part is defined for use within X.400.

e. **CITA Evolution:**

The use of STE for secure fax and its interoperability with STU-IIB compliant systems needs to be monitored.

Group 4 Fax is the digital fax standard which is intended in due course to be the replacement for the analogue Group 3 fax. Group 4 may take some time to grow as it requires the use of ISDN

908. VIDEO CONFERENCING.

a. **Description of Service:** These are standards for transmitting audio and video between CIS. The standards for IS to IS video conferencing are covered under Whiteboarding in paragraph 1705.

b. **Scope of Service:** ITU video and audio standards are only relevant to communications.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement to perform video conferencing.

2. **Openness:** Open standards exist.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Interconnection security policy will often prohibit the direct connection required for IS-hosted video conferencing between nations (as opposed to purely comms-hosted video conferencing).

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope. Video conferencing standards are relevant to the communications systems only.

d. **CITA Specification:**

ITU-T H.320, ITU-T H.221, ITU-T H.242,
ITU-T H.261, ITU-T H.230, ITU-T H.231, ITU-T H.243,
ITU-T H.233, ITU-T H.234, ITU-T H.244.

Implementers should note that the above standards do not guarantee interoperability.

e. **CITA Evolution:**

ITU-T H.323 + ITU-T T.120.

909. GRAPHICAL/STILL IMAGE DATA INTERCHANGE STANDARDS.

a. **Description of Service:** This category covers a wide range of standards used for representation of still image and graphic data.

b. **Scope of Service:** Services are applicable to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement for standardisation of image representation.

2. **Openness:** Many open standards exist.

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** Converters are required to support legacy formats.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:** JPEG version 1.02;

GIF version 89a, July 1990.

It is likely that, for the majority of systems, several additional standards will need to be supported for interoperability with legacy systems (e.g. TIFF).

GIF is a non-lossy format for encoding raster images. It is a proprietary format but the readers carry no royalty obligation. JPEG is a lossy compressed format which is best for encoding high-resolution photographic images. A JPEG-GIF translation capability is required. This is supported by many mainstream drawing/graphics packages; third-party utilities are also widely available. There is no acceptably open standard for editable graphics.

e. **CITA Evolution:**

Although the cited standards are relevant to CITA independently, they are also referenced in standards such as HTML and MIME. Therefore, if these standards change or are extended, the CITA set should be extended accordingly.

The Portable Network Graphics (PNG) format is emerging as replacement for GIF. It is a non-lossy format with much greater compression (though not as high as JPEG); nor does it suffer from the same proprietary restrictions as GIF. Market-place support is growing, hence its status as a standard needs to be monitored.

910. GEOSPATIALLY REFERENCED DATA INTERCHANGE STANDARDS.

a. **Description of Service:** Standards for transfer formats of geospatially referenced data (e.g. overlays).

b. **Scope of Service:** Services are applicable to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement for interchange of geospatially-referenced data (e.g. overlays).

2. **Openness:** De jure format standards may not be completely effective for end-user (desktop) interchange of geospatially referenced data between systems (e.g. DIGEST). De facto product-oriented standards exist in the desktop computer environment and are widely supported.

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** There are many GIS in use in existing systems and significant quantities of GIS data in proprietary formats. Legacy applications software assumes proprietary formats which will require conversion either to other proprietary formats or to less common de jure format standards. Some CITA-conformant systems will need to support additional (proprietary) formats to provide interoperability with specific legacy systems; the legacy systems themselves will dictate where and what additional formats will be needed.

5. **Cost/Risk Issues:** Adoption of a de jure interchange format for geographically indexed data could preclude use of many COTS GIS products, unless partnership with GIS vendors helps to ensure development and maintenance of data interchange converters.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope. The emergence of future standards will need to be monitored and CITA extended to include overlay interchange formats.

d. **CITA Specification:** DIGEST v 2; S-57 edition 3.

e. **CITA Evolution:**

The specific evolving standards selected depend on success of NATO and other initiatives to promote DIGEST (v 2.0 and later versions) as a standard for interchange of geospatially referenced data (i.e. uptake by GIS vendors). The Open GIS consortium (OGIS) is attempting to agree on, among other things, a common set of GIS services and a common data interchange standard. It is supported by all the main GIS vendors and has the potential to produce an acceptably open standard. How far any resultant standards will be adopted and supported is yet to be seen. These developments should be monitored.

911. MOVING IMAGE AND AUDIO/VISUAL DATA INTERCHANGE STANDARDS.

a. **Description of Service:** These are a range of standards used for representation of moving images.

b. **Scope of Service:** All are applicable to the information exchange level of interoperability. ITU Video standards are only relevant to communications systems.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There are inter-nation requirements for some standards listed in this category. There is no evidence of a present inter-nation requirement for transfer of moving images between IS.

2. **Openness:** Open standards exist in most areas.

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

MPEG2 for video (ISO 13818);

PCM for Audio (ISO 11172-3);

CDFS (ISO 9660).

CDFS is required for interoperability via physical media distribution. The CITA standards are those called up in MIME (RFC 1521 and RFC 1522). These are currently:

a. PCM encoding for audio;

b. MPEG for video;

c. JPEG and GIF for still images (see under graphical/still image category).

MIME is likely to evolve to support any future standards that become widely adopted, thus the CITA should track evolution of MIME. In particular, although MPEG is the dominant open standard for moving image and audio-visual at the present time, the uptake and status of other standards needs to be monitored.

e. **CITA Evolution:**

The commercial market place is rapidly adopting the ITU-H.323 and ITU-T.120 standards for multimedia. These standards together cover all aspects of multimedia (and embody many subsidiary standards). They are used by prominent Internet products such as RealAudio and RealVideo.

912. AUDIO DATA INTERCHANGE STANDARDS.

a. **Description of Service:** A range of standards used for representation of sound. Includes various standards relevant to telephony.

b. **Scope of Service:** ITU audio standards are only relevant to communications and are thus applicable to the interconnection level of interoperability. Audio information can be stored and replayed digitally using specific file formats (e.g. .AU, .WAV, AIFF); these are relevant to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is evidence of an inter-nation requirement for transfer of sound between CIS.

2. **Openness:** Open standards exist in most areas.

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

PCM (ISO 11172-3).

e. **CITA Evolution:**

Audio standard selection is conditioned by current de facto multi-media mail standards; evolution of these needs to be monitored to ensure CITA standards remain consistent.

913. FILE COMPRESSION STANDARDS.

a. **Description of Service:** These are standards for the extraction and encoding of compact file representations.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement to exchange compressed data.

2. **Openness:** Many open compression standards exist.

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** Support may not be available on certain legacy systems for compression formats.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope. The CITA should consider all open compression formats (.gz, .zip, .tar, etc.) and specify these instead of the compression utilities themselves.

d. **CITA Specification:**

zip.

e. **CITA Evolution:**

Compression standards applied at the application level generally require specific action by end-users to zip and unzip files. General purpose compression applied at lower level (e.g. IP header and payload compression) may provide a more transparent and scaleable service.

914. MULTIMEDIA AND DISTRIBUTED REAL TIME SERVICE DATA INTERCHANGE STANDARDS.

a. **Description of Service:** All standards under this category are already covered in one of the other data interchange categories. For video, see earlier sections on Graphical/Still Image, Moving Image and Audio/Visual data interchange standards. For audio, see earlier section on Audio Data Interchange Standards.

915. PAGE DESCRIPTION.

a. **Description of Service:** Standards for describing page layouts for submission to print or display devices (e.g. PostScript).

b. **Scope of Service:** Services are applicable to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements exist for transfer of information in device-specific formats (e.g. camera-ready documents and artwork or where an application unique to one CCEB nation needs to pass a printable output to another CCEB nation's system).

2. **Openness:** Proprietary standards exist which have sufficient product and cross-platform support.

3. **Boundary Issues:** Support for designated interchange formats is required at system boundaries only; in all cases, different formats may be used internally.

4. **Legacy Issues:** Many systems will be unable to read, display or print current page description formats.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Some standards allow the inclusion of executable code which could be a security risk.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

1. Primary Standard

   PostScript (Level I and Level II); EPS (both proprietary).

2. Secondary Standard(s)

   PDF.

e. **CITA Evolution:**

None at present.

CHAPTER 10

SYSTEM AND NETWORK MANAGEMENT

1001. SERVICE AREA

Services included in this area are:

a. System management

b. Local Area Network management

c. National Wide Area Network management

d. Coalition Wide Area Network management

1002. SYSTEM MANAGEMENT.

a. **Description of Service:** These are services supporting the management of information systems, including user administration, configuration management, fault management and security management.

There is no evidence of an inter-nation requirement. Open standards do exist (e.g. SNMP) however security policy will usually preclude system management interactions between systems. Special considerations are required for transfer of access control and authentication data between systems. This service area is therefore outside the CITA scope.

1003. LOCAL AREA NETWORK MANAGEMENT.

a. **Description of Service:** These are services supporting the management of local area networks under the control of end-systems.

LAN management is a purely local issue (i.e. not relevant to inter-nation interoperability) hence there is no inter-nation requirement. Also, security policy will usually preclude LAN management interactions between systems. This service area is therefore outside the CITA scope.

1004. NATIONAL WIDE AREA NETWORK MANAGEMENT.

a. **Description of Service:** Services supporting the management of wide area networks within the wide-area communications infrastructure.

National Wide Area Networks will be managed by national staff hence there is no inter-nation requirement. Also, security policy will usually preclude WAN management interactions between systems. This service area is therefore outside the CITA scope.

1005. COALITION WIDE AREA NETWORK MANAGEMENT.

a. **Description of Service:** Services supporting the management of the Coalition Wide Area Network (CWAN).

b. **Scope of Service:** Services are applicable to the interconnection level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a requirement for the management of CWAN. This will typically require an inter-nation group (the Coalition Communications Control Center) having a high level view of the CWAN's connections and performance.

2. **Openness:** No open standards exist.

3. **Boundary Issues:** Centralised system management will ultimately require system administrators to have privileged access rights that transcend system boundaries.

4. **Legacy Issues:** Systems that do not support remote system management must be managed locally.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Allowing system management protocols to pass through system gateways will inevitably weaken overall system security and may not be permitted.

7. **System Evolution:** No significant impact.

8. **Conclusion:** CWAN management at a high level is within CITA scope.

d. **CITA Specification:**

There is no CITA specification at present, however a brief description of the CWAN management is given below.

e. **CITA Evolution:**

None at present.

f. **CWAN Management**

In any federation of systems and networks, the management functions (i.e. network, system, application, and service management) are normally performed by a wide range of individuals, activities, and organizations. These management and/or controlling functions are performed at all levels within the network hierarchy. However, in the CWAN environment, these functions must be performed at the Coalition Communications Control Center (CCCC or Quad C). An alternate Quad C exists to supplement, and provide backup for, the operation of the main Quad C.

The purpose of the Quad C (and its alternate) is to provide seamless, secure information products and services to JWID participants, especially warfighters, in support of decision-making and mission accomplishment.

These centres can be located within any domains. While they can provide virtual presence at any location on the network, each control centre can perform independent and integrated management functions supporting the CIS which provide operational support essential to sustaining the CWAN. The Quad C operational concept is aimed at realigning, consolidating, and integrating these management functions to fulfill the following goals:

- Enhanced C4IFTW support
- Secure operations
- Coordinated problem resolution
- Shared management information (status, availability)
- Global visibility
- Interoperable resources

The Quad C has oversight responsibility for the entire CWAN and interfaces directly with the network participants. It provides the overall management control and technical direction of the CWAN. Its management functions are:

- Fault management
- Configuration management

- Performance management
- Security management

The Quad C is also responsible for the following functional responsibilities and requirements:

- Providing CWAN policy, standards, and guidance for systems and network management;
- Monitoring status, in real-time or near-real-time, of CWAN applications, networks systems, and concerns of the JWID Joint Project Office;
- Providing access to Global CWAN status for authorised users as required;
- Implementing tool suites, processes, and databases that provide the “global” view for applications, systems, and network assets.

More information on the CWAN management can be found in CCEB Publication 1007.

1006. COMMUNICATIONS BEARER SYSTEM MANAGEMENT.

a. **Description of Service:** Services supporting the management of communications systems forming elements of the CWAN.

Communications systems will be managed by national staff hence there is no inter-nation requirement. Also, security policy will usually preclude management interactions between communications systems. This service area is therefore outside the CITA scope.

CHAPTER 11

SOFTWARE ENGINEERING

1101. SERVICE AREA

These are standards for the system/software engineering lifecycle processes. It includes the associated tools and programming environments as well as standards for programming languages and their bindings. They are not relevant to interoperability and are therefore outside the CITA scope. Software engineering services are relevant to other objectives such as software re-use, application portability or value for money.

This page intentionally blank

CHAPTER 12

GRAPHICS

1201. SERVICE AREA

This category includes a miscellany of graphics-related standards, many of which are also listed elsewhere in the guides. For clarity, standards in this category have been grouped into a number of areas which are described separately below.

Services included in this area:

a. Graphics programming languages and APIs

b. Application software packages having a drawing capability

c. Military symbology standards

1202. GRAPHICS PROGRAMMING LANGUAGES AND APIS.

a. **Description of Service:** Languages or language bindings to facilitate the production of graphics-based applications software.

b. **Scope of Service:** Not relevant to CITA objectives. Relevant to application- or person portability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No inter-nation requirement.

2. **Openness:** Not relevant.

3. **Boundary Issues:** Not relevant.

4. **Legacy Issues:** Not relevant.

5. **Cost/Risk Issues:** Not relevant.

6. **Interconnection Security Issues:** Not relevant.

7. **System Evolution:** Not relevant.

8. **Conclusion:** Outside CITA scope.

d. **CITA Specification:** None.

e. **CITA Evolution:** None.

1203. APPLICATION SOFTWARE PACKAGES HAVING A DRAWING CAPABILITY.

a. **Description of Service:** Examples include CAD/CAM packages, OA graphics packages.

b. **Scope of Service:** Not relevant to CITA objectives. Relevant to application- or person portability. OA graphics is covered under Data Interchange.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** No inter-nation requirement.

2. **Openness:** Not relevant.

3. **Boundary Issues:** Not relevant.

4. **Legacy Issues:** Not relevant.

5. **Cost/Risk Issues:** Not relevant.

6. **Interconnection Security Issues:** Not relevant.

7. **System Evolution:** Not relevant.

8. **Conclusion:** Outside CITA scope.

d. **CITA Specification:** None.

e. **CITA Evolution:** None.

1204. MILITARY SYMBOLOGY STANDARDS.

a. **Description of Service:** Standards for representation of military symbols (usually on map overlays).

b. **Scope of Service:** Relevant to CITA objectives. The symbols are relevant to application or person portability and possibly to operational security, however the underlying encoding information, which defines the meaning behind the symbols, is relevant to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements exist to pass symbolic information. This relates to the symbol types (e.g. heavy battle tank, frigate) rather than the actual graphical symbols used to represent them.

2. **Openness:** No open standards exist, though there are military standards which are widely supported by CCEB nations.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** Many systems will not support adopted standards.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** The standardisation of graphical military symbols may be a desirable goal but at present it is only relevant to people or application portability. It is relevant for systems to be able to inform each other of the presence and location of other units. How those units are represented is a matter for individual nations.

d. **CITA Specification:**

MIL-STD-2525A (Symbol codes only).

There is currently no requirement to exchange military symbol sets for interoperability (there are clear requirements for HCI purposes, but this is not relevant to the CITA). However it is important that the encoding of information is agreed CCEB-wide so that sender and recipient have a common understanding of the data content. A common symbol set might be desirable for some combined operations.

e. **CITA Evolution:**

May in future be required to support the exchange of geospatially-referenced data. The requirement for this, in turn, needs to be monitored.

This page intentionally blank

CHAPTER 13

INTERNATIONALISATION

1301. SERVICE AREA

Internationalisation services are those standards and conventions that facilitate the use or re-use of systems or software within different National or cultural contexts. They cover a broad range of Internationalisation standards which can be loosely categorised as character sets, specific data representations and Internationalisation aspects of system interfaces (mainly HCI). These services are largely irrelevant to CITA objectives, with the exception of character sets (which are covered under the data exchange category above). These standards are primarily relevant to people portability.

This page intentionally blank

CHAPTER 14

MESSAGE SECURITY SERVICES

1401. SERVICE AREA

Services included in this area are:

a. Message origin authentication

b. Message access control

c. Message content privacy/confidentiality

d. Message content integrity

e. Certificate management and distribution

f. Message non-repudiation with proof of origin

g. Message non-repudiation with proof of delivery

h. Message security labelling

i. Message accountability

These topics are covered in ACP120 describing a Common Security Protocol. The following sections have been included for completeness.

1402. MESSAGE ORIGIN AUTHENTICATION.

a. **Description of Service:** Service providing assurance that a message was originated by the user indicated as the sender. It is the veritable identification of the user or organisation that originated the message.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a clear inter-nation requirement that the origin of all formal messages can be authenticated.

2. **Openness:** Standards exist in this area (X.509) and five nations within the CCEB have agreed common algorithms for digital signatures (e.g. DSS).

3. **Boundary Issues:** Since a digital signature is formed by encrypting a message digest or hash with a private key, common algorithms and certificate profiles are required if this is to succeed across national boundaries. The binding of the corresponding public signature key to the originator is achieved by the signing of the certificate by the Certification Authority. For certificate path processing to be successful across boundaries, the Certificate Management Infrastructure Authentication Framework also needs to extend across these boundaries.

4. **Legacy Issues:** Users on legacy systems that do not support the use of certificates and digital signatures will be unable to authenticate message origin unless a boundary device is utilised to verify the digital signature of the originator, and mechanisms are employed within the legacy system to guarantee integrity of the message between the boundary device and the recipient. Similarly outgoing messages can have the digital signature of the boundary device appended to provide a level of authentication in the other direction.

5. **Cost/Risk Issues:** Sufficiently strong algorithms are in the public domain, and commercial products are available to implement them. Five nations within the CCEB have agreed on common algorithms for digital signatures. The main cost/risk issue is in the supporting infrastructure for the generation and distribution of certificates and tokens and the cost/risk impact of this aspect may be significant.

6. **Interconnection Security Issues:** No further issues.

7. **System Evolution:** Lack of an acceptable certificate management infrastructure will slow system evolution.

8. **Conclusion:** The current CITA should standardise authentication mechanisms in support of secure message transfer protocols.

d. **CITA Specification:** ACP120 (based on X.509 authentication framework).

It is assumed that individual nations will set in place (or defer to) the appropriate organisation to run and administer one or more certification authorities. Certification authorities are an integral part of the X.509 authentication framework.

COMPUSEC and COMSEC measures independent of the messaging service can provide lower granularity authentication services (e.g. peer entity authentication provided by key possession where link/packet level encryption is employed).

e. **CITA Evolution:** Inclusion of other authentication services (e.g. higher-level network authentication services) is highly desirable in the medium term subject to maturity and market acceptance of relevant products/ standards.

1403. MESSAGE ACCESS CONTROL.

a. **Description of Service:** Services for validating authorisation of the user to originate messages is a national prerogative. The originator should ensure that the lowest common clearance of the communications system, end system and recipient dominate the classification of the message. This is to ensure that messages sent do not violate the security policies of the originating domains. Similarly, the receiving domain must compare the classification of the message with the clearance of the receiving domain. For the purposes of interoperability, this only includes standards for exchange of clearance information and security labels.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** (As for Authentication above.)

2. **Openness:** Standards exist in this area (e.g. X.411).

3. **Boundary Issues:** Common security policies or policy equivalence mappings are required to support this service across boundaries.

4. **Legacy Issues:** Other than communications and intelligence systems, few legacy systems support the use of security labels or the processing of clearance information.

5. **Cost/Risk Issues:** Commercial products today do not implement X.411 with the clearance extensions hence are not regarded as providing sufficiently strong security to meet the military requirement; but they appear to be moving in this direction so the cost/risk impact may be acceptable.

6. **Interconnection Security Issues:** No further issues.

7. **System Evolution:** Lack of acceptable commercial products will slow system evolution.

8. **Conclusion:** The current CITA should adopt:

(a) X.411 security label syntax (i.e. the way the labels are represented when they are exchanged);

(b) security label semantics (i.e. standardise the meaning of security labels) are currently being specified by the INFOSEC ISME For signatures, see Message Origin Authentication. However, given that, unlike NATO, the CCEB is not a treaty organisation, in the past it has been deemed impossible to take this logical step forward.

(c) clearance semantics (i.e. standardise the meaning of clearance attributes) are a subset of the security label and are currently being specified by the INFOSEC ISME.

d. **CITA Specification:**

Syntax of security labels and clearance attributes are currently being prepared by the Certificate Management Infrastructure Working Group of the INFOSEC ISME.

e. **CITA Evolution:**

Apart from security labels, no other access control standards have been identified showing any likelihood of becoming sufficiently widely accepted to permit inclusion within the CITA.

1404. MESSAGE CONTENT PRIVACY/CONFIDENTIALITY.

a. **Description of Service:** Services providing confidentiality of message content exchanged between individual end users.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Three of the five CCEB nations have stated a requirement for per-message confidentiality within message transfers.

2. **Openness:** Open standards exist for options within messaging protocols; SMIME, PCT and ACP 120 support the military requirement.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** Few legacy systems offer security functionality within messaging protocols.

5. **Cost/Risk Issues:** All nations are implementing some type of security (ACP 120, PCT or SMIME) and the cost to implement the necessary mechanisms and management infrastructure for interoperability is likely to be acceptable. Different national policies on encryption may hinder adoption of a common policy.

6. **Interconnection Security Issues:** Significant issues exist including key management and the use of common encryption algorithms.

7. **System Evolution:** Lack of acceptable products will slow system evolution.

8. **Conclusion:** The security policy should specify confidentiality options within messaging protocols.

d. **CITA Specification:** Based on X.509 authentication framework.

e. **CITA Evolution:** Within the scope of the INFOSEC ISME. However, in the future commercial solutions may be acceptable for meeting the above requirements.

1405. MESSAGE CONTENT INTEGRITY.

a. **Description of Service:** Services supporting the integrity of messages exchanged.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements exist for integrity options within message transfers.

2. **Openness:** Open standards exist (e.g. SHA-1, MD5) for options within messaging protocols.

3. **Boundary Issues:** No significant impact, unless the message digest or hash is also encrypted to form a digital signature.

4. **Legacy Issues:** Few legacy systems offer security functionality within messaging protocols.

5. **Cost/Risk Issues:** Sufficiently strong algorithms for integrity are in the public domain, and commercial products are available to implement them. However, when these are combined with encryption to form a digital signature, the main cost/risk issue is in the supporting infrastructure for the generation and distribution of certificates and tokens and the cost/risk impact of this aspect may be significant.

6. **Interconnection Security Issues:** There are significant issues relating to the issuing and management of digital signatures and certificates as well as the adoption of common algorithms.

7. **System Evolution:** The reluctance of nations to decide to implement a Certificate Management Infrastructure will affect system evolution.

8. **Conclusion:** CITA should standardise integrity options within messaging protocols.

d. **CITA Specification:** ACP120 (based on X.509 authentication framework).

Integrity is provided by digitally signing a message digest. This in turn relies on X.509 certificates which rely on PKI.

e. **CITA Evolution:** As commercially available security mechanisms and products continue to develop, they may reach a point where the security services they provide are sufficiently strong to meet military requirements.

1406. CERTIFICATE MANAGEMENT AND DISTRIBUTION.

a. **Description of Service:** Services supporting the management and distribution of digitally signed certificates required to implement:

1. Message integrity and authentication security services;

2. Message content privacy/confidentiality.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements arise from the need to distribute signed certificates from a central issuing authority to a directory which is accessible to individual end-systems, and for individual end systems to be able to verify the authenticity of those certificates.

2. **Openness:** There are open standards for directories (e.g. X.500) and emerging standards for Public Key Authentication Frameworks and Certificate Management Infrastructures.

3. **Boundary Issues:** There are significant boundary issues particularly in relation to directory shadowing, replication and certificate path processing.

4. **Legacy Issues:** Few legacy systems provide the necessary mechanisms.

5. **Cost/Risk Issues:** Automated transfer of signed certificates between systems is an immature technology and represents a significant risk. Current commercial products

are not deemed sufficiently secure. Alternative mechanisms such as cross-certificates are currently being examined.

6. **Interconnection Security Issues:** There are significant issues relating to the generation, distribution, management and user validation of signed certificates.

7. **System Evolution:** The reluctance of nations to decide to implement a Certificate Management Infrastructure may slow system evolution.

8. **Conclusion:** Within CITA scope at present, but may be more realistic to be included in future CITA specifications. National policies need to be monitored to determine applicability of commercial standards and Government variants.

d. **CITA Specification:** X.500 and ACP120 (based on CMI X.509 authentication framework).

e. **CITA Evolution:** In the future commercial solutions may be acceptable for meeting the above requirements.

1407. MESSAGE NON-REPUDIATION WITH PROOF OF ORIGIN.

a. **Description of Service:** Services providing the recipient of a message with proof of its origin. This provides the ability to prove to a third party that a message was released by the originator and will protect against any attempt by the message originator to falsely deny having sent the message. Non-repudiation is essentially a security goal that can be achieved using a number of mechanisms. The use of digital signatures with a Public Key Authentication Framework supported by accounting and audit services contribute towards non-repudiation.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements exist for non-repudiation of message transfers. No other instances of inter-nation non-repudiation requirements have been identified.

2. **Openness:** Open standards exist (e.g. digital signatures) for options within messaging protocols.

3. **Boundary Issues:** Security policy needs to be developed to determine where the non-repudiation security service terminates.

4. **Legacy Issues:** Few legacy systems offer security functionality within messaging or other protocols, however most legacy messaging systems offer this service through procedural controls.

5. **Cost/Risk Issues:** Commercial products implementing ACP 120 are available, and products supporting SMIME are emerging. Cost/risk issues are not expected to be significant.

6. **Interconnection Security Policy:** Significant issues including management of digital signatures and the adoption of common algorithms.

7. **System Evolution:** Commercial products implementing ACP 120 are available, and products supporting SMIME are emerging.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:** ACP120 (based on digital signatures within the CMI Authentication Framework and associated PKI).

e. **CITA Evolution:** In the future commercial solutions may be acceptable for meeting these requirements.

1408. MESSAGE NON-REPUDIATION WITH PROOF OF DELIVERY.

a. **Description of Service:** Services providing the originator of a message with proof of its delivery. This provides the ability to prove to a third party that a message was received by a particular recipient and will protect against any attempt by the message recipient falsely to deny having received the message.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements exist for non-repudiation of message transfers. No other instances of inter-nation non-repudiation requirements have been identified.

2. **Openness:** Open standards exist (e.g. signed receipts with trusted time stamps) for options within messaging protocols.

3. **Boundary Issues:** Security policy needs to be defined to determine where the non-repudiation security service terminates.

4. **Legacy Issues:** Few legacy systems offer security functionality within messaging or other protocols, however most legacy messaging systems offer this service through procedural controls.

5. **Cost/Risk Issues:** Commercial products are available so cost/risk issues are not expected to be significant.

6. **Interconnection Security Issues:** Significant issues including management of digital signatures and the adoption of common algorithms.

7. **System Evolution:** Commercial products are available.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:** ACP 120 (based on digital signatures within the CMI Authentication Framework and associated PKI).

e. **CITA Evolution:** In the future commercial solutions may be acceptable for meeting these requirements.

1409. MESSAGE SECURITY LABELLING.

a. **Description of Service:** Services providing a method for associating security labels with objects in a MHS. This is a subset of Message Access Control (Paragraph 1403).

1410. MESSAGE ACCOUNTABILITY.

a. **Description of Service:** This service provides assurance that messages sent are received by the intended recipient, or permitted alternate recipient. The message originator is notified of any problems with message delivery. This can form a part of overall non-repudiation.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements exist.

2. **Openness:** Some standards do exist.

3. **Boundary Issues:** Security policy needs to be defined to determine where the accountability security service terminates.

4. **Legacy Issues:** Few legacy systems offer security functionality within messaging or other protocols, however most legacy messaging systems offer this service through procedural controls.

5. **Cost/Risk Issues:** Implementation cost and risk will be high if commercial products cannot provide the required functionality and assurance.

6. **Interconnection Security Issues:** Significant issues including management of digital signatures and the adoption of common algorithms.

7. **System Evolution:** Lack of products will affect system evolution.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:** ACP 120 (based on digitally signed receipts and PKI).

Digitally signed receipts are a mechanism for confirming that a message has been received by a specific person or entity. Typically the message recipient will use their private key to sign a hash of the receipt body thus providing the sender with the necessary authentication (of who sent the receipt) and ensuring the integrity of the receipt.

e. **CITA Evolution:**

In the future commercial solutions may be acceptable for meeting these requirements.

CHAPTER 15

GENERAL SECURITY

1501. SERVICE AREA

This chapter deals with security services that are over and above those required to support secure messaging (chapter 0). Further comments regarding the state of security policy and the security services required to support wider interoperability are contained in CCEB Publication 1007.

Services included in this area are:

a. Authentication

b. Access control

c. Key management and distribution

d. Data confidentiality

e. Data integrity

f. Accounting and audit

g. Non-repudiation

h. Security domain mediation

1502. AUTHENTICATION.

a. **Description of Service:** These are services supporting the trusted identification of individual users or groups of users of one system attempting to access services or information provided by another system.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an aspiration in future to be able to provide a CCEB-wide logon with automatic propagation of identity and access rights. Less ambitious inter-nation requirements include:

(a) the ability to co-ordinate the management of user identities, access rights, passwords etc. across systems;

(b) the ability to pass clearances or other privilege attributes (e.g. group memberships) between systems when making access requests.

2. **Openness:** Open standards exist in this area (e.g. X.509), but agreement on the syntax and the semantics of clearance attributes is required.

3. **Boundary Issues:** Security properties at the boundary between systems are strongly dependent upon the mechanisms used internally so any standardisation is likely to have an extensive 'systemic' effect.

4. **Legacy Issues:** Few legacy systems offer any sophisticated security functionality which would make them amenable to interconnection in this way.

5. **Cost/Risk Issues:** Single log-on across heterogeneous systems is an immature area which would represent a risky standardisation undertaking. A lack of commonality in approaches will be an increasingly significant impediment to interoperability. National constraints over system security policies will represent a cost and risk to many projects.

6. **Interconnection Security Issues:** Policy may preclude access or the transmission of security attributes between systems in many cases (e.g. where the systems have different security assurance levels). Proxy servers or boundary/border devices may be the only mechanisms allowed under national security policies.

7. **System Evolution:** Any adopted policy that cannot be supported by commercial products will adversely affect the ability of systems to evolve.

8. **Conclusion:** The current CITA should standardise authentication mechanisms in support of secure inter-networking protocols.

d. **CITA Specification:** None at present.

The conclusion regarding the need for secure internetworking protocols is only valid for a limited set of security architectures (i.e. labelled multi-level or compartmented mode systems). It is judged inappropriate for the CITA to restrict the choice of security architecture in this way. Interoperability would nevertheless be enhanced if all systems adopting the above types of security architectures adopt a common authentication protocol.

Standard (strong) authentication mechanisms based on the X.509 framework are becoming available and openly standardised for web services. Inclusion of authentication services in the

CITA is a prerequisite to many additional interworking services being adopted in the medium term.

Authentication (via key possession) will also be promoted via COMSEC measures implemented in the underlying data communications service.

e. **CITA Evolution:**

Monitoring required of the emergence of strong authentication standards for direct interworking mechanisms. Monitoring also required of the emergence of acceptably open standards for authentication protocols and tokens in support of secure internetworking.

1503. ACCESS CONTROL.

a. **Description of Service:** These are services supporting the promulgation of access rights for service/information exchange between systems based on user identity, role, group, clearance or other privilege attributes. This includes standards for security labels where these are used.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** See authentication section above.

2. **Openness:** As with authentication, the overwhelming requirement to standardise for interoperability can be argued to outweigh the openness disadvantages. CCEB-specific standards will be required in areas such as security classification labelling.

3. **Boundary Issues:** As with authentication, security properties at the boundary between systems are strongly dependent upon the mechanisms used internally and national policies. Translation of certain aspects can take place at boundaries (e.g. security classification labels).

4. **Legacy Issues:** Few legacy systems offer security functionality amenable to interconnection in this way.

5. **Cost/Risk Issues:** Inter-nation access control mechanisms and policies need to be established that do not force all end-systems to adopt a uniform security policy or achieve the same assurance targets.

6. **Interconnection Security Issues:** See authentication above.

7. **System Evolution:** Any adopted policy that cannot be supported by commercial products will adversely affect the ability of systems to evolve.

8. **Conclusion:** The current CITA should standardise security classification labels (i.e. permissible labels and their representation). Standardisation in other areas will be conditional upon a significant shift in the market position of relevant technologies.

d. **CITA Specification:** None at present.

e. **CITA Evolution:**

Extension of security classification labels to some other emerging CITA interworking mechanisms. Otherwise none at present.

Monitoring required of the emergence of strong access control standards for direct interworking mechanisms. Monitoring also required of the emergence of acceptably open standards for authentication protocols and tokens in support of secure inter-networking.

1504. KEY MANAGEMENT AND DISTRIBUTION.

a. **Description of Service:** Services supporting the management and distribution of cryptographic keys.

b. **Scope of Service:** All are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements arise from:

(a) the need to distribute keys from a central issuing authority to individual end-systems. This will be determined by wider government policy;

(b) the need for separate end-systems to access or exchange public keys (e.g. for digital signature purposes). This is a potential CITA requirement.

2. **Openness:** There are open standards in this area. Asymmetric keys can be distributed via PKI and Symmetric Keys can be distributed via EKMS. Nation-specific variants of open standards are under development.

3. **Boundary Issues:** There are several issues in both PKI (e.g. path processing across boundaries) and EKMS (e.g. common Transfer Key Encryption Keys) that need to be resolved before keys can be exchanged across national boundaries.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** Automated transfer of keys and other security attributes between systems is an immature technology and represents a significant risk.

6. **Interconnection Security Issues:** Policy may preclude the transmission of security attributes between systems in many cases (e.g. where the systems have different security assurance levels or processing mechanisms).

7. **System Evolution:** No significant impact.

8. **Conclusion:** National policies need to be monitored to determine applicability of commercial standards and Government variants.

d. **CITA Specification:** None at present.

e. **CITA Evolution:**

The CITA could potentially include key management and distribution schemes for other direct interworking mechanisms.

1505. DATA CONFIDENTIALITY.

a. **Description of Service:** Services supporting the confidentiality of information/services exchanged between systems.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements exist for confidentiality and integrity options within more direct communications mechanisms, such as RPCs and transport layer protocols.

2. **Openness:** Open standards do exist for options in transport protocols via Internet technologies (e.g. SSL, TLSP) may soon provide a solution. Operation of RPC mechanisms through firewalls is still immature.

3. **Boundary Issues:** Security policy needs to be defined to determine where the confidentiality security services terminate.

4. **Legacy Issues:** Link layer encryption has been the traditional means of providing confidentiality services, and few legacy systems offer this service at other layers.

However, even if a common IP high grade crypto is achieved, it will not meet all the requirements for the foreseeable future in respect of availability, transec and traffic flow security, hence there will continue to be a need for high grade link cryptos to meet these requirements.

5. **Cost/Risk Issues:** Inter-nation data confidentiality mechanisms and policies need to be established that do not force all end-systems to adopt a uniform security policy or achieve the same assurance targets.

6. **Interconnection Security Issues:** At present, high grade security for connectivity can only be achieved through link layer encryption. IP based encryption is not yet sufficiently mature.

7. **System Evolution:** S/MIME is expected to evolve to include many of the features specified in ACP 120 and could become a suitable mechanism for application layer confidentiality services for some systems.

8. **Conclusion:** Scope dependent on availability of standards. Confidentiality options within direct interworking mechanisms (e.g. HTTP, RPCs) may be relevant to the medium-term.

d. **CITA Specification:**

Use of ACP 120 application layer data confidentiality or link level encryption.

e. **CITA Evolution:**

There are potential future requirements for data confidentiality options within additional CITA services. Monitoring of the evolution of de facto standards such as S/MIME is required.

1506. DATA INTEGRITY.

a. **Description of Service:** Services supporting the integrity of information/services exchanged between systems. Countering the threat of direct attack, data insertion or modification via exposed communications channels is assumed to be addressed by the data integrity services. These can be provided as part of the underlying data communications service or they can operate at the application layer or other layers within the OSI model. Requirements for integrity options within direct interworking services (i.e. interworking mechanisms other than messaging) depend on the extent to which these services are themselves adopted in the CITA in the medium term.

b. **Scope of Service:** All are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** See data confidentiality above.

2. **Openness:** See above.

3. **Boundary Issues:** See above.

4. **Legacy Issues:** See above.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No further issues.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Scope dependent on the extent to which direct interworking services are adopted in the CITA in the medium term. As for confidentiality above.

d. **CITA Specification:**

Use of ACP 120 application layer digital signatures or link level encryption.

e. **CITA Evolution:**

There are potential future requirements for data integrity options that will support direct CITA interworking mechanisms; however, no applicable open standards can yet be identified. Monitoring required.

1507. ACCOUNTING AND AUDIT.

a. **Description of Service:** These are services supporting the recording and analysis of security-relevant events involved in the exchange of services/information between systems.

b. **Scope of Service:** Services are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement.

2. **Openness:** Open standards exist. Procedure-based mechanisms may need to be adopted.

3. **Boundary Issues:** Audit trails are usually maintained within a system boundary and require applications to produce the necessary logs. Audit logs can be passed across system boundaries (e.g. using SNMP), but national security policies may preclude this.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Security Operating Procedures for Accounting and Audit within nations apply. Audit logs could be passed across system boundaries, however this can weaken security (see below).

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope. Accounting and audit mechanisms can be used locally to support non-repudiation

d. **CITA Specification:**

CITA may need to adopt the CWAN standards and procedures for accounting and audit. Nations will continue to maintain their own services for accounting and audit.

Security is of concern when audit logs are passed through firewalls which typically form the boundary of a system. Management protocols (e.g. SNMP) run over UDP; operating UDP through a firewall will weaken the security it provides.

e. **CITA Evolution:**

Requirements for exchange of accountability data between systems to allow audit of distributed applications. Monitoring is required, both of any emerging commercial standards, and of CCEB requirements.

1508. NON-REPUDIATION.

a. **Description of Service:** These are services to ensure that when information exchange takes place between systems, neither the sender nor the receiver can deny having taken part in it.

b. **Scope of Service:** Services are applicable to interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Inter-nation requirements exist for non-repudiation of information exchange other than messaging.

2. **Openness:** No open standards exist.

3. **Boundary Issues:** Security policy needs to be defined to determine where the non-repudiation security service terminates.

4. **Legacy Issues:** Few legacy systems offer this service other than by procedural controls.

5. **Cost/Risk Issues:** Adoption of a non-COTS solution will increase cost and risk.

6. **Interconnection Security Issues:** No further issues.

7. **System Evolution:** Any adopted policy that cannot be supported by commercial products will adversely affect the ability of systems to evolve.

8. **Conclusion:** Non-repudiation options within information exchange are within scope of the current CITA. However there is currently a lack of standards.

d. **CITA Specification:**

None at present.

e. **CITA Evolution:**

Monitoring of requirement and standards required.

1509. SECURITY DOMAIN MEDIATION.

a. **Description of Service:** Support for the secure exchange of services between systems operating under differing security policies or within separate security domains (e.g. firewalls and guards).

b. **Scope of Service:** All are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** Security domain mediation mechanisms are needed for interoperability but the requirement for them generally arises on a bilateral basis. A future CCEB security policy may give rise to a need to standardise mediation services.

2. **Openness:** No open standards for such services presently exist. Firewall products have a general utility in securing interconnections between end-systems. However, these are not sufficiently well standardised to qualify as being open.

3. **Boundary Issues:** Firewalls typically form the boundaries of systems and are responsible for mediation between the internal system and external WAN environments.

4. **Legacy Issues:** Special enabling mechanisms will continue to be needed to mediate between the security policies of legacy systems.

5. **Cost/Risk Issues:** Building high-assurance guard devices add to cost and risks of interconnection.

6. **Interconnection Security Policy:** The effectiveness of a firewall is dependent upon the mediation rules that it enforces.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside scope of the current CITA. A future CCEB-wide security policy may bring such services within CITA scope.

d. **CITA Specification:**

Awaiting CCEB policy. Policy should develop to ensure coherent domain mediation through nations' firewalls.

e. **CITA Evolution:**

Monitoring required of emergence of acceptably open standards.

CHAPTER 16

SUPPORT APPLICATION SOFTWARE

1601. SERVICE AREA

This category covers general-purpose or utility applications software. A variety of application types could be included under this heading such as office automation, databases and web browsers. However it is the policy of the CITA to not specify applications; indeed it would contravene certain nations' law if it did. Instead the CITA focuses on the interchange formats and service provision standards that such applications should provide.

This page intentionally blank

CHAPTER 17

COLLABORATIVE COMPUTING

1701. SERVICE AREA

Collaborative computing covers a range of services that support group working. The services identified here include a number that are potentially relevant to interoperability. Services included in this area are:

a. Workflow services

b. On-line wide-area publishing services

c. News group services

d. Whiteboarding

1702. WORKFLOW SERVICES.

a. **Description of Service:** Services supporting the automated transfer of documents or other information between users or organisations on the basis of a predefined business process.

b. **Scope of Service:** All are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a possible future inter-nation requirement for workflow services.

2. **Openness:** Open standards are emerging.

3. **Boundary Issues:** The immature status of emerging standards make interoperability at system boundaries difficult to achieve.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope at present because there are no sufficiently open standards. Future requirements, the status of standards from the Workflow Management Coalition[9] and the status of products (e.g. Lotus Notes, SAP & PeopleSoft) need to be monitored.

d. **CITA Specification:** None.

e. **CITA Evolution:** None at present. Requirements for inter-nation exchange of workflow services need to be monitored.

1703. ON LINE WIDE-AREA PUBLISHING SERVICES.

a. **Description of Service:** Services supporting group access (read/write) to structured or unstructured information on the basis of subject area or other categorisation.

b. **Scope of Service:** All are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a requirement for the support of group access but in read-only mode.

2. **Openness:** Open standards exist.

3. **Boundary Issues:** Support for designated interchange format is required at system boundaries only. Different formats may be used internally.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** Write access to on-line published information would need suitable security measures in place.

7. **System Evolution:** Standards are evolving rapidly but new versions are generally backwards compatible.

---

[9] The Workflow Management Coalition, founded in August 1993, is an international organisation of workflow vendors, users, analysts and university/research groups. The Coalition's mission is to promote and develop the use of workflow through the establishment of standards for software terminology, interoperability and connectivity between workflow products. Consisting of over 130 members, spread throughout the world, the Coalition has quickly become established as the primary standards body for this rapidly expanding software market.

8. **Conclusion:** Within CITA scope for read access only. Write access will come within the CITA scope if security issues can be resolved.

d. **CITA Specification:**

1. Primary Standard

HTTP(v1.1)/HTMLv4.0.

2. Secondary Standard(s)

SGML for high value, complex publications.

XML where meta-language data definitions are required.

e. **CITA Evolution:** XML is likely to substantially replace HTML as a browser standard. See document interchange paragraph 902.

1704. NEWS GROUP SERVICES.

a. **Description of Service:** Information transfer services designed to notify registered subscribers of updates occurring in news groups and transfer relevant information.

b. **Scope of Service:** All are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a possible future inter-nation requirement for News group services.

2. **Openness:** Open standards exist.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Policy:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Within CITA scope.

d. **CITA Specification:**

NNTP (RFC 977).

e. **CITA Evolution:**

The evolution of current and compatible standards needs to be monitored.

1705. WHITEBOARDING.

a. **Description of Service:** Services supporting the sharing of displays across a network allowing multiple users to collaborate simultaneously in the creation, review and updating of graphic or textual information.

b. **Scope of Service:** All are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a possible future requirement for Whiteboarding services.

2. **Openness:** Open standards are emerging as the ITU-T T.120 series.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** Most legacy systems will not support Whiteboarding.

5. **Cost/Risk Issues:** Adopting a product that does not comply with the emerging open standards could incur significant subsequent cost penalties.

6. **Interconnection Security Policy:** Supporting Whiteboarding across security boundaries is likely to be prohibited because of the close coupling of user terminals and the lack of security mechanisms.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope at present because no firm requirement yet. Possible future requirements and status of standards and products need to be monitored.

d. **CITA Specification:** None.

e. **CITA Evolution:** Monitoring is required of the emerging standards (ITU-T T.120 series) and products.

There are currently no finalised open standards available, though it is to be expected that when the ITU-T T.120 series of standards are agreed, they will be adopted by the industry. Products are appearing (e.g. Microsoft's Net Meeting, Netscape Conference, Compass) and compliance levels vary. Some are compliant with the communication layer protocols within T.120, but not fully compliant with other aspects of the T.120 set.

This page intentionally blank

CHAPTER 18

CCEB SPECIAL APPLICATION SOFTWARE

1801. SERVICE AREA

This category covers system or mission-specific applications software which would only be expected to be found on systems performing a similar role. Potential relevance to any of the CITA objectives can only really be assessed on a case-by-case basis for these applications. Services included in this area are:

a. Geographic Information Systems

b. Track Management Systems

c. Alert services

d. Data Fusion

1802. GEOGRAPHIC INFORMATION SYSTEMS.

a. **Description of Service:** Applications providing a wide variety of services for storing, manipulating and querying geospatial data.

b. **Scope of Service:** All are applicable to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a requirement to share geospatial data, but no requirement to standardise on an application.

2. **Openness:** Attempts are being made by GIS vendors to develop some standards for APIs and data interchange. Agreement by the Open GIS Consortium (OGIS) on an API standard has now been achieved.

3. **Boundary Issues:** Can avoid standardising on products by adopting interchange formats.

4. **Legacy Issues:** There are lots of legacy applications and geospatial data bases around.

5. **Cost/Risk Issues:** Potentially serious implications if poor product choice is made. Some nations cannot specify a product because of procurement rules.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** GIS data bases can be difficult to evolve or port to newer systems.

8. **Conclusion:** For geographic data exchange DIGEST forms part of the CITA specification as defined in paragraph 910. The decision on whether to adopt the OGIS agreed API depends on market availability.

d. **CITA Specification:** None.

e. **CITA Evolution:**

The take-up of OGIS-agreed APIs and exchange standards needs to be monitored.

1803. TRACK MANAGEMENT SYSTEMS.

a. **Description of Service:** Applications providing services relating to the acquisition, correlation, update and query of tracks.

b. **Scope of Service:** All are applicable to the information exchange level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is a requirement to share track data (and hence a common picture), but no requirement to standardise on an application.

2. **Openness:** There are no open standards for track management services. Military standards for passing track data exist (e.g. OTH-Gold).

3. **Boundary Issues:** Can avoid standardising on products by adopting interchange formats.

4. **Legacy Issues:** Potentially relevant. The wide use of Nauticus as the main track management application could lead to problems if support for the product changes.

5. **Cost/Risk Issues:** Application standardisation may lead to undesirable procurement constraints.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside CITA scope. At present interoperability can only be achieved by specification of a single product. If a suitable data interchange format emerges then there would be no requirement to standardise on a product.

d. **CITA Specification:** None.

e. **CITA Evolution:** Monitor products and standards.

1804. ALERT SERVICES.

a. **Description of Service:** Information transfer services designed to support the rapid or widespread distribution of information, usually having great operational significance.

b. **Scope of Service:** All are applicable to the interworking level of interoperability.

c. **Assessment of Scope for inclusion into CITA**

1. **Inter-Nation Requirement:** There is an inter-nation requirement to pass alerts such as flash messages.

2. **Openness:** No open standards.

3. **Boundary Issues:** No significant impact.

4. **Legacy Issues:** No significant impact.

5. **Cost/Risk Issues:** No significant impact.

6. **Interconnection Security Issues:** No significant impact.

7. **System Evolution:** No significant impact.

8. **Conclusion:** Outside scope of current CITA because there are no open standards. It is deemed desirable for certain alerts to be sent between CCEB nations, particularly in relation to threat warnings. At present, however, there are no open standards and no suitable products.

d. **CITA Specification:** None.

e. **CITA Evolution:** Monitor products and standards.

1805. DATA FUSION.

a. **Description of Service:** It is recognised within the CITA that as coalition forces become more integrated there will inevitably arise the need to fuse data from disparate sources. Such sources of data could be multinational contributing to a truly common operational picture. No standards exist at present hence there is no CITA specification. However it is anticipated that these services could form part of a future CITA.

CHAPTER 19

ABBREVIATIONS

ABCA	American, British, Canadian and Australian Armies
ACP	Allied Communications Publications
ADatP3	Allied Data Publication (Volume) 3
API	Applications Program(ming) Interface
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation.1
C2I	Command, Control and Intelligence
C4I	Command, Control, Communications, Computers and Intelligence
C4IFTW	C4I For The Warrior
CALS	Continuous Acquisition Lifecycle Support (formerly: Computer-aided Logistic Support)
CASE	Computer-aided Software Engineering
CASM	CESG Architecture for Secure Messaging
CCCC	Coalition Communications Control Center (for CWAN)
CCE	Common Communications Environment
CCEB	Combined Communications and Electronics Board
CDDA	Central Data Definition Authority
CD-ROM	Compact Disk Read Only Memory
CDFS	Compact Disk File System
CDMG	Central Data Management Group
CESG	Communication Electronic Support Group

CIS	Communications and Information Systems
CITA	Combined Interoperability Technical Architecture
COE	Common Operating Environment
COMPUSEC	Computer Security
COTS	Commercial Off The Shelf
CWAN	Coalition WAN
DAP	Directory Access Protocol
DBMS	Database Management System
DCE	Distributed Computing Environment
DCOM	Distributed Common Object Model
DDE	Dynamic Data Exchange
DIE	Defence Interoperability Environment
DIE-TA	Defence Information Environment - Technical Architecture
DIF	Data Interchange Format
DIGEST	Digital Geographic Information Exchange Standard
DM	Data Management
DNS	Domain Name Service
DoD	Department of Defense
DTA	Defence Technical Architecture (UK)
EDI	Electronic Document Interchange
EKMS	Electronic Key Management System
EMC	Electromagnetic Compatibility
EPS	Encapsulated PostScript

FY	Financial Year
GIS	Geographic Information System
HCI	Human Computer Interface
HO	Hydrographic Office
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
IEEE	Institute for Electrical and Electronic Engineers
IER	Information Exchange Requirement
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPC	Inter-Process Communications
IPS	Internet Protocol Suite
IS	Information System
ISO	International Organisation for Standardization
IT	Information Technology
ITA	Interoperability Technical Architecture
ITArch	Information Technical Architecture (Canadian)
ITU	International Telecommunications Union
JPEG	Joint Photographic Experts Group
JTA	Joint Technical Architecture
LAN	Local Area Network
LPD	Line Printer Daemon
MIL-STD	Military Standard (US)

Mil Svy	Military Survey
MIME	Multipurpose Internet Mail Extensions
MMHS	Military Message Handling System
MOD	Ministry of Defence
MS	Message Store; Microsoft
MPEG	Moving Picture Experts Group
NATO	North Atlantic Treaty Organisation
NFS	Network File Service
NNTP	Network News Transfer Protocol
NSITA	Nation-Specific ITA
NT	(Windows) New Technology
NTP	Network Time Protocol
NWTDB	Naval Warfare Tactical Database
OA	Office Automation
ODA	Open Document Architecture
ODBC	Open Database Connectivity
OLE	Object Linking and Embedding
ONC	Open Network Computing
OSI	Open System Interconnection
OSIPS	OSI Protocol Suite
OTH-G	Over The Horizon - Gold
PCM	Pulse Code Modulation
PDF	Portable Document Format

POP3	Post Office Protocol (Version) 3
PS	PostScript
QAP	Quadripartite Advisory Publication
QSTAG	Quadripartite Standardisation Agreement (ABCA)
Quad C	Coalition Communications Control Center (for CWAN)
RDA	Remote Data Access
RDBMS	Relational DBMS
RFC	Request For Comment
RPC	Remote Procedure Call
RTF	Rich Text Format
SA	System Architecture
SDH	Synchronous Digital Hierarchy
SGML	Standard Generalised Markup Language
SMB	Server Message Block
SMIME	Secure MIME
SMTP	Simple Message Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSL	Secure Sockets Layer
STE	Secure Telephone Equipment
STANAG	Standardisation Agreement (NATO)
STEP	Standard for Exchange of Product data
TA	Technical Architecture

TBA	To Be Added
TCP	Transport Control Protocol
TLB	Top Level Budget (Holder)
TLSP	Transport Layer Security Protocol
TRM	Technical Reference Model
TSIX(RE)	Trusted Systems Interoperability Group (Restricted Environment)
UDP	User Datagram Protocol
WAN	Wide Area Network
WINS	Windows Internet Name Services
XML	eXtensible Markup Language

CHAPTER 20

GLOSSARY & DEFINITIONS

ALLIED NETWORK

Defines activities entirely within the control of members of a defined set of nations. Within the CITA this is generally accepted to mean the five CCEB nations.

CANDIDATE SERVICES

Classes of functionality within CIS. They also serve as logical placeholders for groupings of standards that share similar attributes of functionality. Each service contains a definition, approximated to the collection of standards contained within it. Each service parallels an industry accepted information technology "functional" area at a broad system service level. Service definitions serve to map functional system support software requirements to specific standards through matching the definition to the standards within.

CITA WORKING GROUP

The working group established by the CCEB Principals to develop the Combined Interoperability Technical Architecture.

COALITION NETWORK

A broader description intended to include any member nation that may form part of a multi-nation activity. Whilst possible to base such activities on Allied requirements it is understood that a less regimental structure will usually apply.

COMBINED INTEROPERABILITY TECHNICAL ARCHITECTURE (CITA)

The Technical Architecture which contains the technical recommendations for a profile of standards and guidelines for support of essential requirements for interoperability among CCEB nations.

COMMUNICATIONS INFRASTRUCTURE

The underlying foundation or basic framework for transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems.

COMPETING DRIVERS

Business and operational imperatives that may influence standardisation, such as devotion of control, avoidance of lock-in, transfer of risk, cost, etc.

DE FACTO STANDARD

Standards that are widely used but which have not been through an open standards-making process leading to a *de jure* standard. Often they will be proprietary standards implemented in popular commercial products.

DE JURE STANDARD

Standards that have been developed by a formal process of drafting, review and agreement at National, European or International levels.

EMERGING STANDARD

A specification that is under consideration by the CITA working group, but has not completed the process of approval by the group. Emerging standards are often subject to significant change prior to approval.

INTEROPERABILITY

a. The ability of CIS from different CCEB Nations to interconnect, interwork and exchange meaningful information in a secure and timely fashion as determined by business/operational imperatives (CCEB Publication 1007).

b. The ability of two or more systems to exchange information and to mutually use the information that has been exchanged (IEEE P1003.0/D18).

INTEROPERABILITY LEVELS

The following levels of interoperability are defined:

a. **INTERCONNECTION.** End-systems are capable of direct electronic attachment to one another or to a common logical network.

b. **INTERWORKING.** Interconnected systems employ compatible mechanisms for the exchange of services and data.

c. **INFORMATION EXCHANGE.** Users and applications on different, interworking systems can attach a common meaning[10] to data exchanged between them.

LEVELS (ENTERPRISE, NATION, PROJECT)

a. **ENTERPRISE -** The full domain of the CCEB which consists of the following nations: United States, United Kingdom, Australia, New Zealand, and Canada.

b. **NATION -** A CCEB country, e.g. New Zealand.

c. **PROJECT -** The focused implementation of a specific requirement.

NATIONAL NETWORK

Defines those operations performed entirely within the control of a single nation and whose operation does not impact upon the international environment.

OPEN SOLUTION (OPEN SPECIFICATIONS)

A standard or specification that is controlled and maintained by a public body. Also includes Publicly Available Specifications (PAS).

SERVICE

A logical entity within the Information Technology Environment that performs an overall agreed upon function.

STANDARD

A document, established by consensus and approved by an accredited standards development organisation, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order and consistency in a given context (IEEE P1003.0/D18).

---

[10] This is not restricted to metadata definitions and models but includes any data that contains information that must be interpreted in order to be understood by humans or applications (e.g. OA and HTTP format tags).

STANDARDISATION

An activity that consists of the process of formulating, issuing guidance on and implementing standards (ISO/IEC Guide 2:1996).

LIST OF EFFECTIVE PAGES

Subject Matter	Page Numbers	Change In Effect
Title Page	I (Reverse Blank)	Original
Foreword	III (Reverse Blank)	Original
Letter of Promulgation	V (Reverse Blank)	Original
Record of Changes and Corrections	VII, VIII	Original
Record of Pages Checked	IX, X	Original
Table of Contents	XI to XVI	Original
Chapter 1	1-1 to 1-18	Original
Chapter 2	2-1 to 2-12	Original
Chapter 3	3-1 to 3-2	Original
Chapter 4	4-1 to 4-2	Original
Chapter 5	5-1 to 5-8	Original
Chapter 6	6-1 to 6-14	Original
Chapter 7	7-1 to 7-10	Original
Chapter 8	8-1 to 8-6	Original
Chapter 9	9-1 to 9-20	Original
Chapter 10	10-1 to 10-4	Original
Chapter 11	11-1 to 11-2	Original
Chapter 12	12-1 to 12-4	Original
Chapter 13	13-1 to 13-2	Original
Chapter 14	14-1 to 14-10	Original
Chapter 15	15-1 to 15-10	Original
Chapter 16	16-1 to 16-2	Original
Chapter 17	17-1 to 17-6	Original
Chapter 18	18-1 to 18-4	Original
Chapter 19	19-1 to 19-6	Original

ACP 140

Subject Matter	Page Numbers	Change In Effect
Chapter 20	20-1 to 20-4	Original
List of Effective Pages	20-5 to 20-6	Original
Index	20-7 to 20-8	Original

INDEX

ACP 140

ORIGINAL